



SYNAPTIC
LABORATORIES LTD.

Ronald Kelson
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

Benjamin Gittins
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

Synaptic Laboratories Ltd.
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Wednesday, 31 March 2010

Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks

PART 1 - Covernote

In 2009-2010 the European Network and Information Security Agency (ENISA) <http://www.enisa.europa.eu/> made a call for Scenario Proposals on Emerging and Future Risks.

One proposal was then selected for study in 2010 in the area of Trust and Privacy. In this area ENISA was looking for proposals to identify major risks in the area of trust, security and privacy posed by new and emerging technologies and applications. ENISA restricted scenario proposals from including proprietary technologies. Synaptic participated in this Call with a scenario focused on the risks associated with the global dependency upon Public Key Cryptography (PKC) and Public Key Infrastructure (PKI). Synaptic proposal, as included in this document, satisfied all ENISA's submission requirements and was shortlisted by ENISA.

We are placing a copy of the submission online for the benefit of those who may have an interest in PKC dependent systems (SSL/TLS, SSH, SSL-VPN etc) and PKI. The writing style selected for the submission was chosen to hopefully make the issues more accessible to a wider, non-technical audience.

According to Article 3(a) of Regulation 2004/460, ENISA fulfils the task of collecting appropriate information in order to analyse current and emerging risks. It concentrates on risks at the European level, which could produce an impact on the resilience and the availability of electronic communications networks as well as on the availability, integrity and confidentiality of the information accessed and transmitted through them. ENISA provides the results of the analysis to Member States, the Commission and other stakeholders.

Synaptic originally submitted to ENISA a long version of our scenario, totalling some 56 pages with citations. This had to be reduced to a 3 page submission, to satisfy the ENISA guidelines. An anonymous version of the 3 page submission entitled: "*The risks of continued EU dependency on PKI and PKC*" was eventually reviewed by members of the ENISA Permanent Stakeholders Group.

In this web article the 3 page version (which appears below before the main document) can be considered as an executive summary of the longer document, which is entitled: *“The risks to current, emerging and, future technologies which rely on Government approved standards-based public key technologies with their known risks of catastrophic failure and potential to create cyber war, caused by the presence of multiple existing single points of potential trust failure, whereby one player can compromise the entire global system and the known future risks from code breaking quantum computers.”*

The 56 page submission provides a scenario on three distinct stages in the life of “John Smith”, a hypothetical UK identity management security expert working in the international Aerospace and Defence sector. John’s eyes and thoughts provide us an opportunity to explore a series of events in a way that sheds insight into the underlying technical issues facing the European (and at times global) community.

The first stage is set in the present, the second stage in 5 years, and we show how decisions made in stages one and two can extrapolate out in a third stage set in 9 years. The submission then goes on to outline the rationale and significance of our proposed scenario including information on current and emerging US and EU research and development agendas.

The submission ends with a section outlining the empowering benefits to the EU (global) community of a comprehensive risk management report on PKI and an easy-reference table of the 90 different threats and issues under 8 headings identified within the submission. Extensive citations are embedded as footnotes throughout the long version document.

Synaptic has been actively researching and designing cybersecurity solutions to address many of the risks and issues identified in this ENISA submission. Six Synaptic proposals have been accepted and advanced by the US National NITRD Cybersecurity Summit (August 2009). Papers on the Synaptic proposals will be presented at the Cyber Security and Information Intelligence Research Workshop <http://www.csiir.ornl.gov/csiirw/> in April 2010 and at the IEEE Key Management Summit <http://2010.keymanagementsummit.org/> in May 2010.

We trust that you find our submission to ENISA to be of value in your own risk management processes.

We welcome any comments on this ENISA submission and any enquiries about our proposals to protect PKC/PKI from the identified threats.

Benjamin Gittins and Ronald Kelson



SYNAPTIC
LABORATORIES LTD.

Ronald Kelson
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

Benjamin Gittins
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

Synaptic Laboratories Ltd.
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Wednesday, 31 March 2010

Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks

PART 2 -

3 Page (Executive Summary) Submission to ENISA's Call for Scenario Proposals on Emerging and Future Risks

The risks of continued EU dependency on PKI and PKC.

Submission to ENISA's Call for Scenario Proposals on Emerging and Future Risks

1. Working Title:

The risks of continued EU dependency on PKI and PKC.

(Original title:

The risks to current, emerging and, future technologies which rely on Government approved standards-based public key technologies with their known risks of catastrophic failure and potential to create cyber war, caused by the presence of multiple existing single points of potential trust failure, whereby one player can compromise the entire global system and the known future risks from code breaking quantum computers.)

2. Stakeholder Group:

Industry

3. Impact Area:

Trust and Privacy

4. Target audience:

All stake holders in public key cryptography (PKC) and public key infrastructure (PKI) including User Groups, System Administrators, Certificate Authorities, Critical Infrastructure Projects (CIP), Legislators, European Commission, Research Community, Co-ordination Action programs, National Security Agencies.

5. Brief outline of proposed scenario:

Efficiencies demand greater interconnectivity in all (inter)national (PKI dependent) ICT systems. By 2015 single point of trust weaknesses in PKI are exploited. Cyberfraud now >1,000 BEuro annually. An arms race ignites around quantum cryptanalysis. With mounting PKI failures and no PKI succession planning, the EU Internal market is destabilised as public confidence in eCommerce and eGov plummets. More laws demand the use of PKI dependent biometrics. Countries trade biometrics and increase citizen surveillance.

Note: Citations and further technical references are available in our 56 page supporting document (found in part 3)

6. Rationale / Significance of proposed scenario

The problems with PKC and PKI are « *understood as issues already visible as possible future risks to network and information security* » and present a « *significant risk of undermining the smooth functioning of the Internal Markets* ». Below we outline how our scenario has « *security problems already identified as global issues* » and that « *there is a need for closer cooperation at global level to improve security standards, improve information, and promote a common global approach to network and information security issues* ». Critically, international co-operation is required for **PKI Succession Planning** to prevent destabilisation of the Internal Market, prevent market fragmentation, and generally to protect EU interests. **Today's PKI architecture has already been found wanting** and, according to unchallenged expert opinions published in documents generated by U.S. Cyber Security Initiatives, today's PKI is also considered a significant barrier to the universal adoption of cryptography which is now believed necessary to increase cybersecurity and mitigate fraud and identity theft. **There is an increased threat** as a consequence of emerging global tensions and the escalation in the development of cyber war capabilities resulting in an increased sophistication of the perpetrators, whether they are nation states or individuals. There are no super powers in cyber space, with modern technology and readily available hacking tools every citizen is powerful. **There is increased criticality** because the emergence of the Internet has shifted more economic and social activity online, making security virtually synonymous with cybersecurity.

Global single point of trust failures exist in the architecture of the civilian PKI which enables any of the 20+ PKI Root Certificate Authorities to generate malicious certificates against any website address (based on the results of the MD5 Rogue Certificate Authority Attack). Today approximately 86% of fraud happens by management at a level against their own organisations. This is significant given that current PKI architecture is vulnerable to insider attackers. **The Internet is becoming increasingly Militarised by Governments.** The U.S. Air Force is advocating Cyber War. The U.S. has already conducted cyberwar in IRAQ with attacks that exploited the mobile phone network. **Weakness in PKI and PKC are likely to be exploited during cyberwar.**

The United States captures the biometrics of everyone entering their country. **Biometrics are already being traded internationally by the United States and other countries.** Biometrics will be increasingly combined with CCTV systems by law-enforcement agencies, effectively resulting in a **civilian panopticon**. Biometric data does not change significantly over the life time of an individual, however ECRYPT has small confidence in existing algorithms and key lengths beyond ten years, particularly for asymmetric algorithms (ECC, RSA, D&H) that protects biometrics. Archived biometric data could be widely exploited in the medium term. Increased risks typically lead to increased monitoring. **Comprehensive Internet surveillance would complete the civilian panopticon vision.**

The RSA algorithm currently protects a billion applications. PKI currently protects transactions worth trillions and investments worth tens of billions. With the massive momentum built up around the deployment of the 20th century security solutions using PKI, at-risk PKI is the main contender to protect all the latest European Government ICT initiatives and major infrastructure projects such as SESARJU (30 year operational life). Projects using PKI (or likely to use PKI) include (international, national and cross Government) ID initiatives including (eGovernment, UK NIS, e-Passports, FP6 STORK), Aerospace (SESARJU, Galileo) and other Government projects (CIPHER Project, UK ICT Strategy). In fact most Government and Civilian ICT systems critically rely on at risk PKI for security. **ECRYPT advise that they have little confidence in PKC (RSA, ECC) 10 years into the future.** The EU, US, and China Governments are funding research into code breaking quantum computers. To quote Prof. Seth Lloyd: “*The National Security Agency, which supports research in quantum computing, candidly declares that given its interest in keeping U.S. government communications secure, it is loath to see quantum computers built. On the other hand, if they can be built, then it wants to have the first one.*” If just one (open or closed) quantum computing research project is successful, that group can provide code-breaking and forgery services to Governments, national intelligence organisations, military organisations, or terrorists anywhere in the world. **There will be significant instability and liability shifting if this happens.**

US NIST has stated “*that in the light of quantum computing Cryptographic Key Management system designers MUST look at means other than using public key-based key management systems*”, so that these systems can achieve “*resilience against quantum computing attacks*” (2009). There is new legislation being rapidly advanced in the USA today that would require the US NIST to lead the USA's international cybersecurity standards. New Identity Management, Key Management and cyberspace security standards may become weapons of coercion and not tools of global social empowerment for the 98% of the world's population that is not .gov, or .mil. Without international participation at the highest level, without a system of checks and balances, global identity management issues may not be addressed in a way that is appropriate to the European or global civilian community.

SECOQC advises that current QKD networks are not suitable for use as large scale public networks such as the Internet. An attack recently eavesdropped 100% of a quantum cryptographic key due to weakness due to a photon detector vulnerability in modern QKD deployments. **This leaves only symmetric key technologies such as AES-256.**

7. Benefits

THE EU COMMUNITY IS MARGINALLY SECURE TODAY – THE EU COMMUNITY IS TOTALLY UNPREPARED FOR THE FUTURE COMPUTING TECHNOLOGIES THAT IT IS DEVELOPING

Current and immediate future benefits (Public Key Infrastructure & Single point of trust failure)

1. The report would provide an **authoritative, independent establishment and confirmation of the known weaknesses of PKI**. It would **highlight the unacceptable risks and ramifications of relying on security systems with system wide single-point-of-trust failures** that can negatively effect, and potentially destabilise, the entire EU community.
2. The report would **mitigate continued non-action by calculating and articulating the risks and potential negative impacts** from the loss of security and privacy, and the roll-on negative economic impact to EU Nations and stake-holders as a result of not immediately addressing the known weaknesses posed by PKI.
3. Once we are able to consider **the mean failure cost for each stakeholder** (which is the cost we expect to incur as a result of the lack of security), this loss **can be balanced against the cost of improving system security**. In this way a well-formed risk assessment report can provide an estimate of an appropriate amount to spend to address the known threats.
4. A risk management study **would support the existing EU calls (FP6 SecureIST) for the development of a universally acceptable hardened information technology infrastructure** that can provide MEDIUM to LONG-TERM assurances (50-to-100 years).
5. The outcome of such a study by ENISA on PKI **would feed into the Unified Identity Framework proposed by the RISEPTIS, and influence the design of security mechanisms in the €2.1 Billion SESARJU development efforts** and could potentially influence every segment of the European and the electronically connected Global community.
6. The ensuing benefits from a report that **instigates change in the EU Community includes a vastly improved ICT security infrastructure for future sensitive and valuable computer applications, systems with higher availability, greater survivability from targeted attacks, improved stability during periods of aggressive behaviour by any nation providing a certificate authority**. That is, ICT systems implemented with adequate levels of information assurance reduce their vulnerability to cyber attack and do not promote cyber war escalation. Consequently, **there will be less dependence on invasive surveillance and development of cyber-attack capabilities as deterrents**.

Short-Medium Future benefits (Public Key encryption & Quantum Computers)

7. The additional benefits from a report which instigates change in the EU community with respect to quantum computer attacks is:
 - a. **a significant reduction in the amount of intellectual property/sensitive personal data that will be at risk of exposure,**
 - b. **a reduction in the severity of ICT exposure to real-time attacks against access control systems,**
 - c. **the avoidance of reworking expensive EU funded critical infrastructure projects from known anticipated attacks, and**
 - d. **improved design and reduced operational costs** by avoiding rip-and-rapidly-replace scenarios that would otherwise occur by non-action today.

With regard to PKI and quantum computing, in our opinion, it is a risky strategy for the EU to aggressively fund codebreaking research and development without adequately preparing for the arrival of these machines. This is particularly the case given quantum computing research has the potential to negatively effect the data security of every European citizen, or to be used as an ICT weapon to attack other countries.

We are not suggesting that the fundamental research into quantum computing should be reduced, or slowed, particularly as this is an internationally competitive research agenda which may offer other non-military benefits. What we are arguing is that there needs to be a focussed PKI risks/threats/costs/benefits study to inform decision makers and lead to adequate guidelines within EU funded research and development programs to address the known risks. By way of example, the previous EU call for 50-to-100 year security (by FP6 SecurIST) was ignored and utterly ineffective in inducing change of behaviour within any segment of the EU community. To our mind it is incomprehensible that the EU has not funded, at least to an equivalent level, the RESEARCH, DESIGN, DEVELOPMENT and DEPLOYMENT of appropriate low-risk countermeasures at the READY to ensure the global community can protect against the negative side-effects of the EU research initiatives in quantum computing. It will take major systems such as EMVCo more than ten years to migrate to a new security paradigm, when one becomes available! The lack of redundancy, distributed trust and resilience in PKI infrastructures are major risks that are compounded by the code breaking quantum threat.



SYNAPTIC
LABORATORIES LTD.

Ronald Kelson
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

Benjamin Gittins
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

Synaptic Laboratories Ltd.
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Wednesday, 31 March 2010

Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks

PART 3 -

Full 56 Page Submission to ENISA's Call for Scenario Proposals on Emerging and Future Risks

The risks to current, emerging and, future technologies which rely on Government approved standards-based public key technologies with their known risks of catastrophic failure and potential to create cyber war, caused by the presence of multiple existing single points of potential trust failure, whereby one player can compromise the entire global system and the known future risks from code breaking quantum computers.

Submission to ENISA's Call for Scenario Proposals on Emerging and Future Risks

1. Working Title

The risks to current, emerging and, future technologies which rely on Government approved standards-based public key technologies with their known risks of catastrophic failure and potential to create cyber war, caused by the presence of multiple existing single points of potential trust failure, whereby one player can compromise the entire global system and the known future risks from code breaking quantum computers.

2. Stakeholder Group

Industry

3. Impact Area

Trust and Privacy

4. Target audience

Legislators, European Commission, Research Community, Coordination Action programs.

5. Brief outline of proposed scenario:

The next 9 years in the life of a security expert

5.0 Executive Summary

Our message is simple:

1. Today, PKI protects transactions worth trillions and investments worth tens of billions. Almost the entire globe is betting the whole shop on PKI; [PKI-001]
2. PKI is a brittle single layer of defence with many known complex problems and limitations; [PKI-002]
3. The global cryptographic community knows that Government standards based PKI could catastrophically fail within ten years, but in spite of this risk and the many single points of potential critical failure, the EU continues massive PKI rollouts even in long term (10-30+ year) critical infrastructure projects; [PKI-003]
4. The community has not yet fully comprehended the extent of PKI dependency, the range of risks and threats, and the complexity of the international issues. This failure results in the continued dependency on PKI and the lack of corrective action which in turn threatens core EU principles, EU Market future, and EU stability; [PKI-004]
5. Preventing cyberwar and cyberfraud (valued at 1,000 billion USD per annum by the FBI) are now at the top of the agenda, and the USA has already started a major project to look for improvements and alternatives to PKI as part of its massive cybersecurity initiatives. [PKI-005] The issue of finding a replacement to PKI affects all of Europe. [PKI-006] A PKI replacement must be balanced so that it takes into account the legitimate interests of all stake holders and does not favour the (political, commercial, military) interests of any one nation or group. [PKI-007] A PKI replacement must be internationally acceptable to enable inter-operability of future global ICT systems. [PKI-008] For these reasons the study of the problem/s in PKI, and the negotiation of the requirements for an international PKI replacement, is beyond the scope of any one EU nation or organisation or major project such as SESARJU. It demands and deserves the full attention of the EU.
6. A risk assessment study is required to survey the known PKI issues and evaluate their potential impact on stakeholders in the EU community. Short term, mid term and long-term technical, research and policy risk treatments need to be proposed to ensure that current security deployments are bolstered and future security deployments enhance the European agenda rather than further jeopardise it.

In this section we present a scenario that addresses the requirements identified as relevant to ENISA¹. Our multi-stage scenario is set over 9 years which «*analyses Current and emerging risks*» from the use of public key cryptography (PKC) and public key infrastructure (PKI) that:

1. Are «*understood as issues already visible as possible future risks to network and information security*»; and
2. Present a «*significant risk of undermining the smooth functioning of the Internal Markets*»

This scenario highlights how the PKI «*security problems identified are a global issue*» and that «*there is a need for closer cooperation at global level to improve security standards, improve information, and promote a common global approach to network and information security issues*» to prevent market fragmentation.

We have set the future scenario over a period of 9 years to demonstrate how decisions taken, or indeed not taken, in the present, could have an exponential impact at a later date. The entire scenario is supported with extensive citations. We identify 90 different issues in 8 subjects. We cross reference these 90 different issues as they occur in the text using [square brackets]. These issues are listed in tabular form at the back of the document for ease of reference.

Our scenario highlights the growing massive global reliance upon public key cryptography in an array of critical applications. In fact the RSA algorithm is now claimed by RSA Security to be deployed in MORE than one billion applications world wide. The rate and range of deployments in both Government and commercial applications continues to build momentum. This continues in spite of the known, complex and potentially catastrophic risks and limitations. [PKI-009] When this momentum and complexity is considered in the context of the constraints caused by the current harsh economic times, it is obvious that it is not economically viable for a security company to research, develop and trial new solutions, even to protect against potentially catastrophic known risks, unless there is already an identified buyer. [PKI-010] For the same compelling reasons, the buyers similarly do not want to fund this type of project, particularly in the absence of clear leadership from Government and industry concerning the critical issues of interoperability and standards compliance [PKI-011]. Therefore there are multiple reasons why an EC level approach must be taken to the study of the PKI issues.

Today's PKI architecture has been found wanting² and, according to unchallenged expert opinions published in documents generated by U.S. Cyber Security Initiatives, today's PKI is also considered a significant barrier to the universal adoption of cryptography which is now believed necessary to increase cybersecurity and prevent fraud and identity theft.

There is an increased threat as a consequence of emerging global tensions and the escalation in the development of cyber war capabilities resulting in an increased sophistication of the perpetrators, whether they are nation states or individuals. There are no super powers in cyber space, with modern technology and more readily available hacking tools every citizen can be a super power.

There is increased criticality because the emergence of the Internet has shifted more economic and social activity online, making security virtually synonymous with cyber security.

There is increased vulnerability because emerging computing paradigms such as networking, distributed computing, and mobile/pervasive computing open wide security gaps that are hard to control.

Our scenario highlights how the lack of adequate research and analysis on these known risks can trigger a chain of side-stepping and liability shifting [PKI-012]. Ultimately, the known risks we describe apply to (practically) all ICT security systems, and some were already being described as a “*nightmare*” as early as 2004³. There exists the potential for countless amounts of past and present secure data being exposed and a vast array of critical systems put at operational risk [PKE-001].

¹ Regulation (EC) no 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (text with EEA relevance). In Official Journal L 077 (13 March 2004), pp. 0001 – 0011. Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

² P. Gutmann. *Everything you Never Wanted to Know about PKI but were Forced to Find Out*. Available at <http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf>

³ Buchmann, J., Coronado, C., Doring, M., Engelbert, D., Ludwig, C., Overbeck, R., Schmidt, A., Vollmer, U., and Weinmann, R.-P. *Post-quantum signatures*. Report 2004/297, Cryptology ePrint Archive, October 2004. Available at <http://eprint.iacr.org/2004/297>

In the United States the National Institute of Standards and Technology (NIST) has already placed cryptographic key management firmly on the US and future international cybersecurity agenda (see section 6.4.3 below) [PKI-005]. NIST has already instigated a project to begin to address the problems, with a call for designers to look at new and different solutions that do not use public key cryptography [PKE-002]. Europe must co-ordinate with the US efforts or, as we will show, massive fractures in the international markets can occur [PKI-013].

We will highlight in our scenario the known security problems/risks/threats that exist as a result of this dependency on public key cryptography, and discuss the impact on current, emerging and future technologies and how their reliance on PKI can negatively effect the global community. We will touch on the complex issues of international identity management, biometrics and the use of PKI as a core enabling technology in these applications.

We also show how the study of PKI can be applied constructively to address and resolve the risks whereby many countries seek to be a single point of control over all data exchanged [SPOTF-001], [SPOTF-002], including data of citizens from other countries, that falls into its possession, without any international distribution of trust or resilience. A new model of international distributed and shared trust with redundancy can be evolved that helps to remove the multiple single points of control and potential catastrophic failure that exist in many of our IT systems today and that in many cases can be exploited today against a citizen or to wage cyber war.

Our scenario focuses on three distinct stages in the life of “John Smith”, a hypothetical UK identity management security expert working in the international Aerospace and Defence sector. John’s eyes and thoughts provide us an opportunity to explore a series of events in a way that sheds insight into the underlying technical issues facing the European (and at times Global) community. The first stage is set in the present, the second stage in 5 years, and we show how decisions made in stages one and two can extrapolate out in a third stage set in 9 years.

This is a possible scenario of the future that can be avoided if action is taken now.

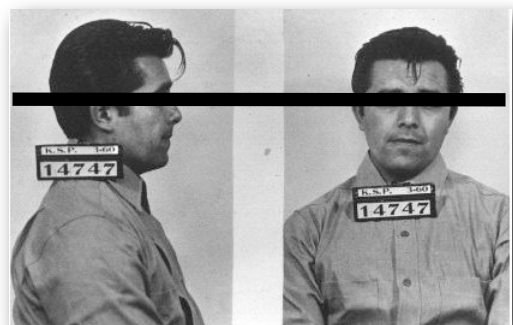
The EC should, in the near term, perform a comprehensive cost/benefit analysis, including the immediate, mid term and long term risks arising from the use of standards based public key cryptography in cybersecurity. This would be invaluable data to inform current and future large EU projects. It should clarify and quantify the risks, it should outline a preferred development path forward, and it should make recommendations on the preferred mechanisms, process and European representative body to lead the necessary international co-operation effort. This effort would be timely, as the USA has already rapidly advanced new draft Federal Legislation that will require the US NIST to lead the USA’s international efforts and activities towards creating new international cybersecurity standards.

5.1 Scenario: 2010 (Current Risks)

John, a cryptographic and identity management expert of 30 years of age, is waiting in a chair at the National Identity Service (NIS) customer centre located at London City Airport. Today John will be applying for a UK National Identity Card (NIC) and updating his ICAO MRTD e-Passport. John, like most people, is feeling a little apprehensive, about what he is about to permit to take place.

John’s passport will expire in about two years however, he has been told that it would be *highly desirable* if he took the opportunity to have a biometric passport ready for his new aerospace security job at Thales. John has recently applied for the position at Thales and was advised he will be given the job on the condition of his identity credentials and background security check passing. John has applied to work on the Single European Sky ATM Research (SESARJU) project during its €2.1 billion development phase. John has been short-listed for the position due to his experience which includes working on the aerospace and defence Transglobal Secure Collaboration Program (TSCP) identity management project⁴.

Today the NIS will capture and permanently archive John’s biometric data including 10 fingerprints, a photo of his face from the front and the side, and his signature. John knows this is exactly the set of biometrics that they capture when enrolling convicted criminals into prison [BIO-001], which makes him wonder if he has just enrolled himself into some similar controlled environment for non-law breaking citizens? [BIO-002] (Image to right is public domain)



⁴ <http://www.tscp.org/>

Like many people, it is not just the initial discomfort in the *process* of capturing of his biometrics and its similarities with the criminal justice process that concern John – it's also the many risks associated with what can happen with his biometrics *after* his details are captured.

In particular, John understands that access to his biometrics will be controlled using public key cryptography. John has closely followed the most recent US cryptographic key management initiatives, so he is aware of many of the known risks that threaten all PKI dependent applications.

John knows that the US NIST has already called for designers to search for key management solutions that do not rely on public key encryption (PKE) and which are resilient against quantum computers [PKI-014]. He knows it is a fact that quantum computers may grow to a size that will catastrophically break all existing deployed public key cryptography (PKC), encryption and digital signatures, possibly within ten years according to some quantum computer experts [PKE-003]. He also knows that in 2009 Google announced⁵ that they were already achieving some better results using the hardware provided by quantum computing company D-Wave Systems Inc. Since biometric (and other) data will be archived and cannot be changed obviously during his lifetime [BIO-003], John wonders at the sense in protecting biometric data (and trillions in transactions and tens of billions in investments) with PKI, since it offers no redundancy and relies on brittle cryptographic algorithms (such as RSA and D&H) that are known to be at risk of complete failure [BIO-004]. However, putting that to one side for now in 2010, John has other concerns.

John recalls sitting at a presentation during the 2008 Annual Smartcard & Electronic Identification Congress and Exhibition (CARTES) in France⁶ when Kathleen Kraninger (illustrated to the right⁷) spoke.

Kathleen, the then Deputy Assistant Secretary for Policy at the Department of Homeland Security, openly disclosed how the United States *actively encourages sharing of biometrics with other countries* [BIO-005].

John, a little taken back by the one sided short discussion on international trading of biometrics, which did not identify any of the risks of international trading in biometrics, followed up later to confirm that he had heard correctly.

To quote a testimony⁸ made before the US House Appropriations Committee, Subcommittee on Homeland Security on “biometric identification”:



“To ensure we can shut down terrorist networks before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Just as we are improving the way we collaborate within the U.S. Government to identify and weed out terrorists and other dangerous people, we have the same obligation to work with our partners abroad to prevent terrorists from making any move undetected.” ... “So what is next? We need to aggressively pursue innovation. Those who want to do us harm continue to contemplate ways to exploit our weaknesses, so we cannot afford to slow down.” ... “We recognize that with the power of biometrics and a foundation of international cooperation, we can transform and enhance the way the people travel the world and the way we protect our nations from those who would do us harm.”

⁵ Neven, H., Denchev, V. S., Drew-Brook, M., Zhang, J., Macready, W. G., and Rose, G. *Nips 2009 demonstration: Binary classification using hardware implementation of quantum annealing*. Tech. rep., GoogleBlogs, December 2009. Available at http://www.google.com/googleblogs/pdfs/nips_demoreport_120709_research.pdf

⁶ <http://www.cartes.com>

⁷ kathleen.kraninger@dhs.gov – Image Courtesy of <http://2002-2009-fpc.state.gov/fpc/113944.htm>

⁸ Kraninger, K., and Mocny, R. A. *Testimony of deputy assistant secretary for policy kathleen kraninger, screening coordination, and director robert a. mocny, us-visit, national protection and programs directorate, before the house appropriations committee, subcommittee on homeland security, “biometric identification”*. Testimony, Rayburn House Office Building, March 2009. Available at http://www.dhs.gov/ynews/testimony/testimony_1237563811984.shtm

Again, the emphasis was clearly on the claimed benefits, but there was no reference to the risks. As of mid-2008, the FBI's biometrics database alone held 56 million prints⁹. Apparently the recent increase in prints is not due to an explosion in crime or terrorism, but more fingerprinting in the private sector. The FBI now processes prints from teachers, bank employees and other non-criminals. *"That is our growth business,"* says Debbie Chapman, who works in the FBI data centre. US State and Federal legislation, such as the Patriot Act and Border Safety Transportation Act, are also driving expansion, remarks Thomas E. Bush 3rd, who served as Assistant Director of CJIS until earlier this year. *"We're seeing literally daily different legislation that requires fingerprint-based background checks."* Biometrics is also moving to military detainees. *"Right after 9/11, we began fingerprinting people in Guantanamo and started exchanging those fingerprints with other countries,"* Bush says. *"In one example, we found out of the first 100 fingerprints we sent to one country, we had three identifications in that country's criminal history database."* And that is precisely the future of biometrics: linking different systems, particularly international databases. *"It will be the international connection,"* Bush says. *"These systems will be connected by biometrics in the not-too-distant future."* John knows all these connected systems will be PKI dependent.

Wondering how extensive the international sharing was today, John found the following article ¹⁰:

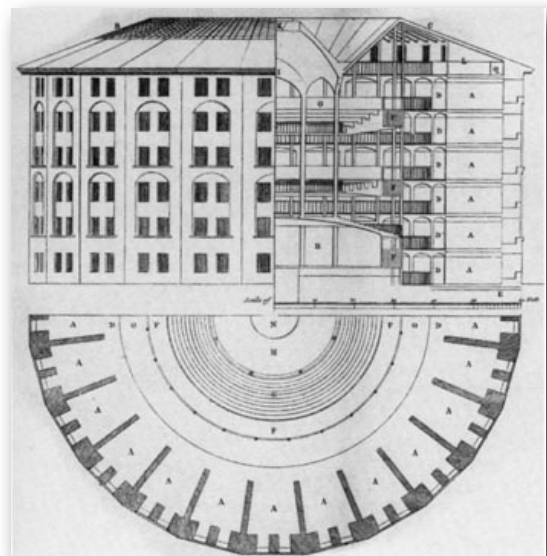
"Miller, (a consultant to the Office of Homeland Defense and America's security affairs) said the United States has bi-lateral agreements to share biometric data with about 25 countries. Every time a foreign leader has visited Washington during the last few years, the State Department has made sure they sign such an agreement."

With India alone planning to capture the biometrics of 1.2 billion citizens¹¹ [BIO-006], John can't help but think there are going to be a lot of biometric linked "trading cards" for Government agencies to play with.

John travels internationally regularly on business, so he knows that if it's not his home country quietly trading his biometrics without his knowledge, it might be another country. America systematically captures the biometrics of everyone entering the United States. [BIO-007] John knows that it is only a matter of time before his biometrics may soon be traded internationally. John wonders if they will tell him at the U.S. airport or at any other foreign location where his biometrics data is accessed or captured, how they will use and share his biometrics? [BIO-008]

John knows ultimately he has no control over where his biometrics might go, or how they might be used. They might be used in identity fraud against him [BIO-009], or his employer, or others, for illicit systems access, funds transfers, Government and corporate espionage or for IP theft purposes. John is also aware that the definition of *"a dangerous person"*, or *"terrorist"*, is very flexible and open to different political interpretation [PAN-001], not just from country to country, but also between different parties in his own country. John also knows that the data could be exploited by others as a tool in cyber warfare. These are all important issues to John, particularly as he appreciates the importance of his employment in the security industry, and also because he has ambition to rise to very senior posts during his working career.

Even in his own country John has concerns about how the data might be abused at some future time. By correlating John's mobile phone cell data in combination with extensive CCTV networks and facial recognition systems supplied with his biometric data, it may not be possible, in the near term future, for John to move outdoors in city areas with any privacy from Governments [PAN-002]. *(Image of original panopticon prison to right is public domain)*



⁹ http://www.aviationweek.com/aw/jsp_includes/articlePrint.jsp?storyID=news/SCAN110509.xml&headLine=U.S.%20Builds%20Largest%20Biometric%20Database

¹⁰ Magnuson, S. Defense department under pressure to share biometric data. In NationalDefenseMagazine.org (January 2009), NDIA. Available at <http://www.nationaldefensemagazine.org/ARCHIVE/2009/JANUARY/Pages/DefenseDepartmentUnderPressureToShareBiometricData.aspx>

¹¹ <http://uidai.gov.in/>

The concept of the original panopticon design (illustrated to the right for use as a prison) is to allow an observer to observe (-opticon) all (pan-) prisoners without the prisoners being able to tell whether they are being watched, thereby conveying what one architect has called the "*sentiment of an invisible omniscience.*"

John wonders if he has just enrolled himself into a global citizens 'prison' with eventually any number of possible invisible controllers, where the multitude of Governments potentially accessing his personal data may now or in the future have very different motivations about its storage and use.

With a shudder, John recalls the Report of the Defense Science Board Task Force on Defense Biometrics¹²:

"Often, it is wise to protect, sometimes even to disguise, the true and total extent of national capabilities in areas related directly to the conduct of security-related activities. This is a classic feature of intelligence and military operations; it also potentially applies to biometrics." ...

"We may expect that biometrics-based tools and techniques will be increasingly deployed in sensitive applications, and used to achieve important successes in support of national objectives. In so doing, we must seek to preserve the security of what the intelligence community calls 'sources and methods,' even while being able to headline the outcomes of such use when otherwise deemed appropriate."

John can think of a lot of reasons that this doctrine may also apply to military advances in quantum computing and attacks against PKI.

Similarly to the brittle nature of ICT systems protected primarily by encryption, where if the encryption algorithm fails there is no resilience or possibility of recovery from the theft and exploitation of past recorded secure data, John also understands that any one of those Governments could become a single point of critical failure in the safe storage and 'correct' use of his own personal biometric data [BIO-010].

"Department of Defense policy should tilt toward saving the 'original' biometric (in high resolution) rather than relying only on the processed metric/template."

– On Defense Biometrics (2006)

John also knows that his biometric data will be used as part of access controls in both his employment and personal life to secured programs, services, data and restricted areas. If his raw biometric data is in the hands of other nations and their agencies, as a result of trade or simple international travel, might this biometric data be used¹³ to attack critical systems? [BIO-009] And as the community becomes trained to provide biometrics on a routine basis, it is easier for attackers to acquire it.

John is concerned that he may be implicated in illicit actions through the use of his biometrics, and depending on the scenario, conceivably he may not be able to convince others that he was not the perpetrator. Similarly to brittle encryption defences, there can be no recovery from the theft and misuse of biometrics. Biometrics are not like a compromised password, they cannot be changed. John wonders how his entire life might be affected if his biometric data was misused. It is becoming an increasingly biometric dependent world, and he can imagine the difficulties he could face in the future with respect to his freedom of access and movement if his biometrics become compromised. Clearly if they were misused, then the authorities concerned for security reasons would probably need to notify an unknown list of other national agencies and potentially foreign Governments, and as far as John was aware there was no recovery process other than for him to be placed on a biometric 'black list'.

John tries to put this line of thought into another perspective in his own life. John wonders if his attendance at a noisy but lawful political demonstration in Ireland calling for greater transparency and accountability in the UK Government when he was 20 years old might be brought up some time in the future and cause him employment problems. After all, according to a Guardian newspaper article¹⁴, the UK Police in 2009 were funded £9m to log 'domestic extremists'.

¹² Defense Science Board (DSB). *On defense biometrics*. Unclassified report of the defense science board task force, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, Washington, D.C. 20301-3140, September 2006. Available at <http://www.acq.osd.mil/dsb/reports/ADA465930.pdf>

¹³ Slashdot. *Hacker Club Publishes German Official's Fingerprint*, Available at: <http://hardware.slashdot.org/article.pl?sid=08/03/29/1941206>

¹⁴ Lewis, P., Evans, R., and Taylor, M. Police in £9m scheme to log 'domestic extremists'. In www.guardian.co.uk (October 2009). Available at <http://www.guardian.co.uk/uk/2009/oct/25/police-domestic-extremists-database>.

Allegedly, detailed information about the political activities of campaigners is being stored on a number of overlapping IT systems, even if they have not committed a crime. It is not hard to imagine that a future Government might consider *anyone* in physical attendance at a political demonstration as a potential radical (terrorist). John recalls the well documented COINTELPRO (an acronym for Counter Intelligence Program) series of covert, and often illegal, projects conducted by the United States Federal Bureau of Investigation (FBI) aimed at investigating and disrupting dissident political organizations within the United States between 1956 and 1971¹⁵. Not surprisingly the FBI's stated motivation at the time was "*protecting national security, preventing violence, and maintaining the existing social and political order.*"

John values a reasonable balance between individual freedom and social responsibility. John was acting on his own principles when he chose to participate in the political demonstration in Ireland. Now, with hindsight, he feels the weight more fully of a civil liberty issue he considered while a student at university:

"Whoever is uncertain if divergent kinds of behavior will be recorded at any time and this information will be stored permanently, used or passed on, will try not to attract attention by these kinds of behavior. Whoever expects that e.g. the attendance of an assembly or the participation in a civic action group will be registered by the authorities and that this will probably cause risks, may probably abandon their corresponding fundamental rights (Art. 8, 9 GG). This would not only impact the individuals' chances for development but also the public interest because self-determination is a necessary condition for the functionality of a liberal democratic polity which is based on its citizens' ability to act and to participate."

– from the German Federal Constitutional Court census Judgement of 1983 as quoted in the article "Current Legal Issues on Video Surveillance" contributed to the SECURITY Congress 2000, Oct. 9-12, 2000 in Essen by Dr Thilo Weichert.

If the authorities or media have archived footage of the demonstration John attended then John knows it will be possible to systematically identify all participants at a later date.

John notes that extraordinary conditions can sometimes lead good people in an organization to rationalize inappropriate behavior. Systems need to be designed to mitigate inappropriate behaviour from occurring, for example through models that offer redundancy and distributed trust, and that enable the detection of inappropriate behaviour when it does occur [SPOTF-003]. Entrenched systems may also invite potential for abuse and may need to be replaced. John is aware that ~65% of fraud in Europe is perpetrated by senior management¹⁶ [SPOTF-004]. Sometimes an entirely new system is required to provide the desired properties, such as has occurred with country wide taxation systems in the past.

So, given everything that he knows about the risks and limitations of PKI itself, and how easily PKI reliant systems such as biometrics could be miss-used, John wonders if he is making the right decision to allow his biometrics to be captured now. From a personal perspective, he knows it will help him win his new job, but just as clearly his compliance can be read as agreement with and support for a security regime that clearly has serious flaws. [BIO-011]

A relaxed, attractive and socially outgoing male customer service representative approaches John and shakes his hand. "Aaron's my name, how are you? Got all your documents?" John is noticeably put at ease by Aaron's sociable personality. With a nod of John's head, Aaron offers to arrange John a coffee and walks him to a private booth. They sit down and a coffee arrives shortly.

Aaron shuffles through some papers and, after noting that all the paperwork is present, begins to speak: "As a British Citizen working in aerospace I confirm that you are eligible to be an early adopter of the new NIS card. Did you know the card acts as a passport when you're travelling within the European Economic Area (EEA) and Switzerland, and that you can buy age-restricted items, such as alcohol, DVDs or video games as the card proves your age without revealing private information like your address?"

John smiled politely.

¹⁵ Hoover, J. E. Counter Intelligence Program (COINTELPRO). Comprehensive information available at <http://en.wikipedia.org/wiki/COINTELPRO>, 1956-1971.

¹⁶ Aguilar, M. K. Profile of a fraudster: Subtle, senior, and stealthy. In www.complianceweek.com (May 2007), Available at <http://www.complianceweek.com/article/3327/profile-of-a-fraudster-subtle-senior-and-stealthy>

Aaron continues: “*And John, you will be glad to know that these card lock you as an individual to one identity through use of details like your name, address and fingerprints, so they’re also highly secure.*”¹⁷

John thinks, “*Secure for who, and secure from what?*” but knows he really doesn’t have much choice about this process, and it is common popular thinking that people who do not want to provide personal data must have something to hide, and so he keeps his thoughts to himself.

Of course John knew the issues surrounding the security of the system itself were much more complicated than Aaron was probably told, or cared to know, and this was not the place or time to argue. John, like many people, was well aware of the controversy around the security of e-Passports and the UK National Identity Card. However, John as a cryptographic expert had a deeper appreciation of what the complications were, for example **the problems surrounding the use of public key cryptography (PKC) in these systems.**

As previously indicated, John understood that PKC was a brittle single line of defence that offered no resilience or recovery [PKE-004], and that civilian PKI systems could be exploited by several parties to create cyber war or to conduct fraud [PKI-015]. John also understands that the UK NIC, as with all ICAO MRTD passports, employs the use of an RFID chip and is designed so that passport control points can query the chip offline. This is promoted as a feature that allows the checking system to validate the credentials just by talking with the Radio Frequency ID (RFID) chip. However, there is a catch. The complication is one of key and certificate management. John is aware of the 2009 US NIST Cryptographic Key Management Workshop that identified various limitations with current cryptographic key management, but this is a special example [PKI-016]. With over 183 countries issuing ICAO passports, and in theory, each country acting as their own Root Certificate Authority (RCA), and each RCA having several dependent Certificate Authorities, there are a lot of public keys and certificates to manage. To simplify the checking process, the RFID chip *helpfully* supplies a copy of the public key that signed the document details to the document reader device. If the reader/terminal does not go online, or has not previously gone online, and VALIDATED that this public key certificate it received from the RFID chip was indeed issued by the specific country that the passport claims to be from, then it becomes possible for any party to forge the electronic identity and electronic biometrics held within an e-passport.

The forging of identity credentials with attacker-supplied digital signatures has been convincingly demonstrated. [PKI-017]¹⁸

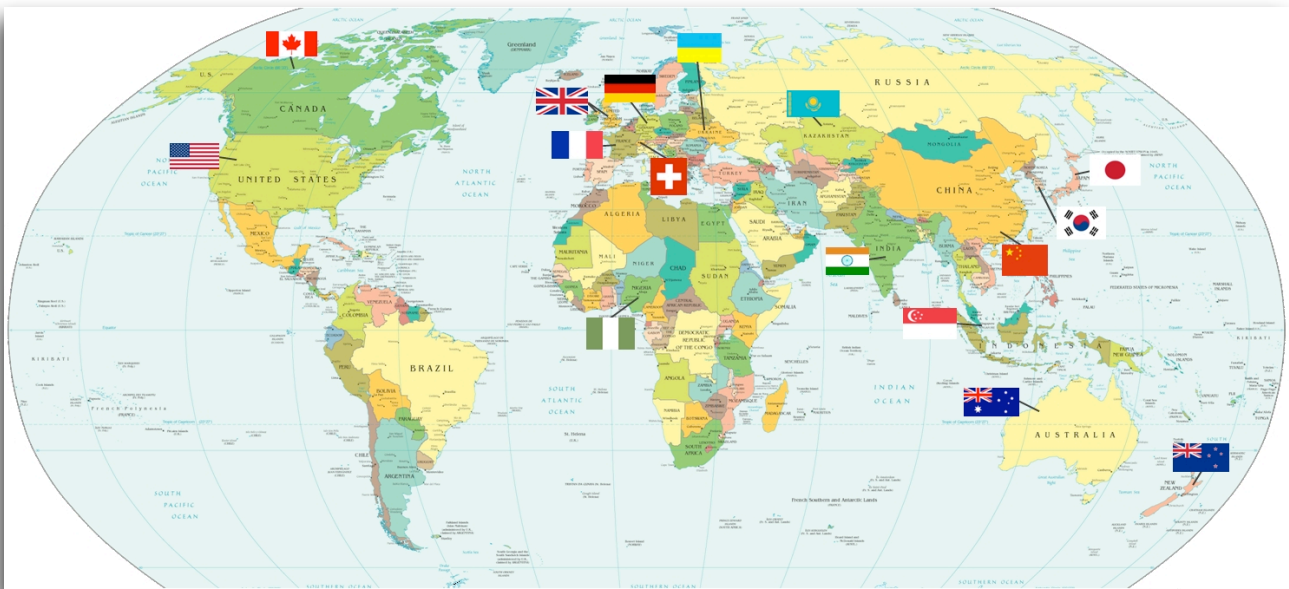
For now John has no choice but to assume, rightly or wrongly, that there is no existing code breaking size quantum computer in existence. John knows that by 2004 there were already more than 150 public quantum computing research projects and that one of the primary reasons for QC research is because of their proven capability to break codes, particularly PKC. John has his reasonable doubts about whether or not the arrival of the first such computers will ever be announced to the public due to its significance to national security. No doubt the person or group or nation state with control of or access to such a computer will wish to maximise its advantage. From a different perspective, a public announcement would be highly unlikely to happen because John can imagine the impact on public confidence and markets if such a computer was announced. For example, all confidence in eCommerce and eGovernment and digital certificates would evaporate, since they are totally dependent upon PKC.

To return to the issue of the critical role of PKI dependent digital certificates in the ICAO Machine Readable Passport scheme, John knows that each of the 183 ICAO members are responsible for managing their own public key certificate authority, and each ICAO member must also have all the public keys for the certificate authorities of the 182 other members. When John last checked (2010), only a very few countries (less than 17 as illustrated below¹⁹) were maintaining and making their keys available on a centrally administered database of public keys.

¹⁷ <http://idsmart.direct.gov.uk/index.html>

¹⁸ Boggan, S. ‘fakeproof’ e-passport is cloned in minutes. In www.timesonline.co.uk (August 2008), Times Newspapers Ltd. Available at <http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>

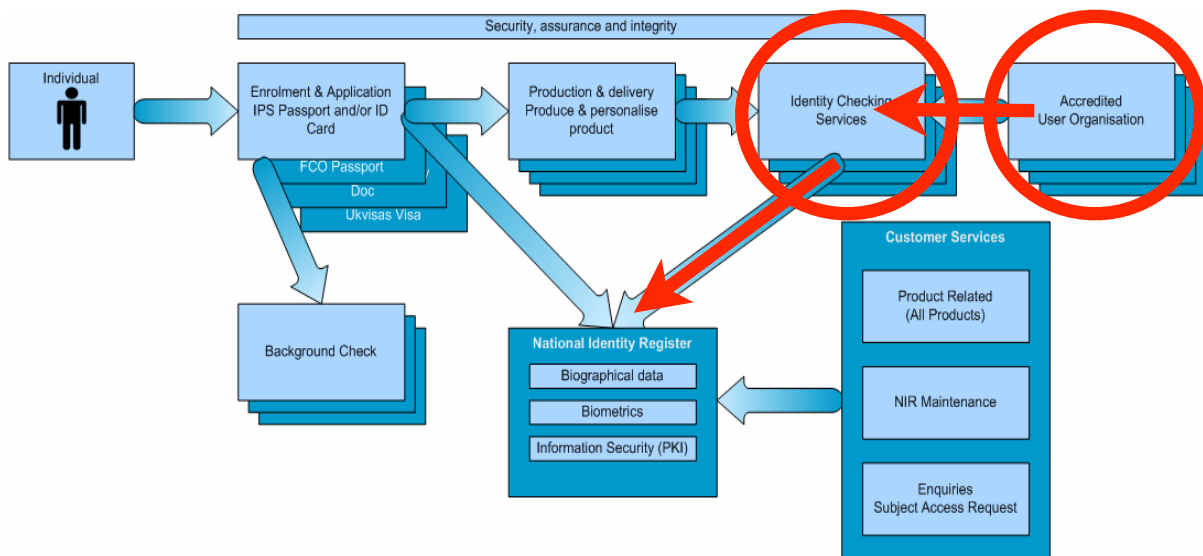
¹⁹ Courtesy of ICAO - <http://www2.icao.int/en/MRTD/Downloads/PKD%20Documents/PKD%20World%20Map.jpg>



Therefore, in a global scenario, most electronic international passport checks cannot be electronically validated with the issuing country, and therefore electronic forgery is possible as has already been conclusively proven [PKI-017].

One of the important ways the UK NIC scheme increases security is by offering a “Passport/Card Validation Service”²⁰ that allows any UK company to check “online” the identity details on the passport/card against the data stored on the UK National Identity Register, for a fee.

John was unable to determine from the Home Office Identity & Passport Service website if this service is accessible to foreign organisations such as border control.



To gain this increase in protection, an organisation seeking to validate that John’s ID has not been forged has to have business processes and accounts in place to check back with the National Identity Registry (as illustrated above with the two red arrow²¹). This step to detect fraudulent cards in the UK NIC scheme is an improved security solution over the ICAO system. It is interesting that added feature completely side-steps the Public Key component of the ICAO scheme. This clearly demonstrates that the NIC architects determined that the public key cryptography used in the ICAO passport/card itself in this application is not adequately secure. [PKI-018]

²⁰ http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/34.htm

²¹ NIS Strategic Supplier Framework Prospectus, 2007. Image and document available at: http://www.securitydocumentworld.com/client_files/070809_nis_strategic_supplier_framework_prospectus_v2_2.pdf

However, this added measure only shifts and partially addresses one of the known PKI risks, because presumably the link between the “Accredited User Organisation” and the “Identity Checking Services” is protected using Public Key Cryptography. It is also likely that the link between the “Identity Checking Services” and the “National Identity Register” is protected using Public Key Cryptography. We note that the diagram above clearly shows that the National Identity Register uses PKI for “Information Security”.

Even if the Aerospace and Defence public key infrastructure (CERTIPATH/TSCP) is used (as opposed to the Civilian PKI structure such as Verisign), the system will continue to have single-point of trust failures within the certificate infrastructure, and the system will still be vulnerable to code-breaking quantum computer attacks.

Furthermore, if the diagram accurately portrays the system, there is no “separation of powers” within the “National Identity Register”, nor the presence of a powerful independent audit body monitoring the activities of the NIR. This raises data privacy and data integrity concerns from insider attacks (administrators or even senior management).

John notes to himself that this type of centralised biometric data storage system cannot be deployed across Europe because some EU member States, such as Germany, do not permit the collection and storage in one location of all a citizens personal data due to risks of potential abuse. For John this is just another example of the international complexity that must be addressed when the risk/cost/benefit analysis of the European and indeed global dependency upon PKI is eventually studied, making it clearly as it were a ‘whole of EU’ project.

To return to the UK NIC Customer Service Centre, John acquiesces and “voluntarily” permits his biometrics to be captured so that, in exchange, he can travel more easily internationally and in order for them to be used for employment and other identification purposes. Next, his biometrics are then transmitted back to the National Identity Register. John’s biometrics will be used to create his National Id Card, and to create his ICAO Machine Readable Travel Document. Both documents use biometrics, and their security mechanisms, will be considered valid for a period of 10 years. [BIO-012]

John knows that some people think that ten years is a solid margin of time for a document to remain secure. However ECRYPT has repeatedly advised that they have little confidence in public key cryptography 10 years into the future.

So, John is not alone when he already anticipates that perhaps in the future there may be stronger e-passport schemes. However, applying stronger security in the future will be too late to protect against some catastrophic attacks. John knows that data today is easily recorded as it travels over private or public networks. Since this archived traffic will include his unchanging biometric data, therefore today’s security must offer resilience against attack for John’s entire lifetime, not just for ten years.

John thought, at any time in the future, an attacker only needs to break the security protecting his **current** passport and related archived traffic to be able to steal and exploit secure data, including his unchanging biometric information. [BIO-013] John knows that this fact actually encourages hackers to record currently secure data, in what are called ‘wait-and-see’ attacks, whereby the hacker could auction this data to the highest bidder, particularly later when the security becomes obsolete and easily breakable [PKE-005]. This worries John because he expects that his biometrics will be used for the rest of his life. He has ambitions to rise to a very senior position during his career, which he expects will involve gainful employment for another 40 years. Then, when he retires, John expects that access identity controls, for example to his pension fund and Government social security services, will make use of his biometrics. In the context of his hoped for and potential lifespan of 100 years, a ten year security margin with low assurance thereafter makes little sense to John [BIO-003], particularly when stronger security options are already available.

John now leaves the UK National Identity Service Customer Centre and travels by train back to his home. John uses the train as it reduces his carbon footprint and it gives him time to either think about identity management issues or share more time with his 4 year old daughter and his partner when they travel together. In his new employment, John will be working on the SESARJU identity management and cryptographic key management technologies. This will be a very difficult project if they really try to address the known risks and threats. He knows the aerospace community (through the TSCP organisation) has spent approximately 5 years working just to reach agreement on how to apply the standards for an international identity management project and creating a secure email standard²². This new standard specifies how to implement the *existing* US Federal Processing security standards. [PKI-019] The TSCP/Certipath public key infrastructure, which uses public key certificate authorities, extends the US Federal PKI system²³. Will the

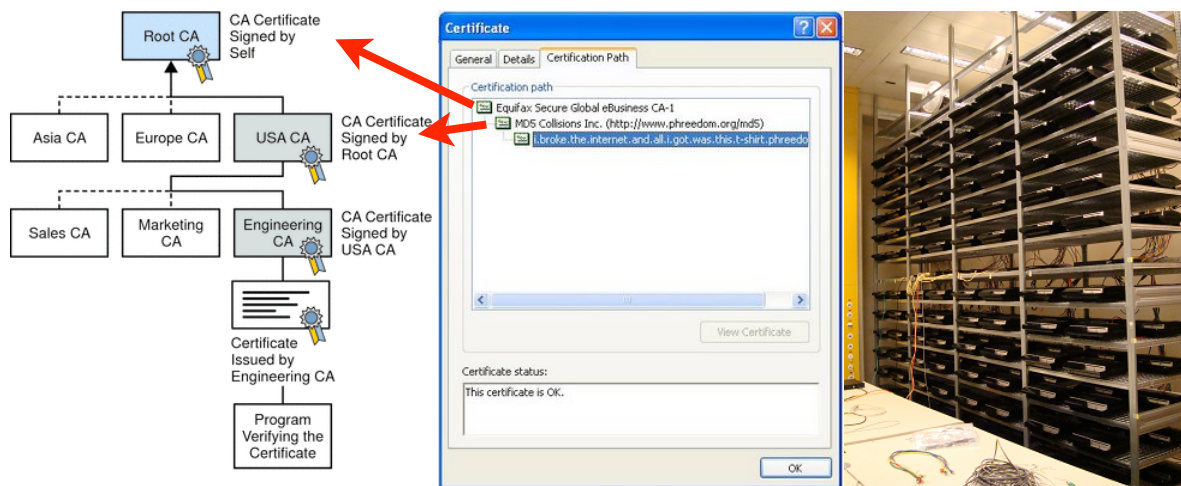
²² Certipath. TSCP, international aerospace and defense industry secure e-mail capability. Version 2.1, CertiPath LLC, August 2008. Available at <http://www.tscp.org/pdfs/SecEmlTechSpecv2-1GR.pdf>

²³ <http://www.idmanagement.gov/fpkipa/>

SESARJU managers determine that it falls within the projects mandate to take cognisance of the latest findings of the US cybersecurity initiatives and address the known risks and threats, or will they take the cheaper and faster option of just adopting the best security solutions currently available, which will mean continued PKI dependency? Given the complexity and international scope of the issues and risks, it is unreasonable to expect one project, even a large one such as SESARJU or Galileo, to tackle a ‘whole of Europe’ problem. Thinking more about SESARJU, John knows that the new air traffic control systems will be extensively exploiting cyberspace. For example GPS services will supplement and in some cases may replace radar, and so cyber security will be even more critical for the safe operation of this 30+ year critical infrastructure project.

With these complex issues and concerns in mind, John now recalls the United Nations Telecommunication Union Chief’s warning in 2009 of the risk of the next world war being in cyber space, a space with no super powers, as every citizen can be a super power²⁴. [CYBER-001] He is aware of the growing, important US cybersecurity initiatives that are beginning to address these issues, and in particular he is thinking about the ease with which the civilian identity name space (such as the Internet Top Level Domains²⁵, ²⁶) management could be exploited to create cyberwar. [PKI-015]

John is recalling the MD5 Rogue Certificate Authority attack²⁷, where a group of civilians were able to exploit a cryptographic weakness in the certificate authorities of several Root Certificate Authorities, including a RCA managed by VeriSign. What grabbed his attention more than the cryptographic weakness was **how they were able to then exploit this fault to make and provide a fake certificate on ANY website on the planet to any civilian Internet user** (Firefox, Internet Explorer, Safari, ...) [PKI-020]



The middle panel above shows a forged Certificate, which is accepted by the Windows Operating System which states: “This certificate is OK.” See MD5 Collisions Inc. (<http://www.phreedom.org/md5>) The right panel shows the cluster of Sony Playstation 3’ devices that were used to find the MD5 collision which led to the rogue Certificate Authority, which in turn could generate fake certificates for any website on the Internet.

Putting aside the technical weakness in MD5, John is wondering how and why the global Internet public key infrastructure architecture was designed with a global/system-wide single point of potential trust failure that permitted one mistake/vulnerability to expose every participant on the Internet? [PKI-021]

²⁴ Walker, G. ITU chief stresses need for cooperation to protect cyberspace. In United Nations Radio (October 2009). Article available at <http://www.unmultimedia.org/radio/english/detail/83203.html>, audio: <http://downloads.unmultimedia.org/radio/en/ltd/mp3/2009/n-itucyberspace.mp3?save> and <http://downloads.unmultimedia.org/radio/en/ltd/mp3/2009/n-touere2.mp3?save>.

²⁵ http://en.wikipedia.org/wiki/Top-level_domain

²⁶ <http://www.iana.org/domains/root/db/>

²⁷ Stevens, M., Sotirov, A., Appelbaum, J., Lenstra, A., Molnar, D., Osvik, D. A., and de Weger, B. M. M. *Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate*. In CRYPTO ’09, vol. 5677 of LNCS, pp. 55–69. Available at <http://eprint.iacr.org/2009/111> see also <http://www.win.tue.nl/hashclash/rogue-ca/>

“Anyone who selects a public CA on a factor other than price fails to understand the trust models that underlie today’s use of CAs.”

—Lucky Green ²⁸

John then asks himself, given that VeriSign comprehensively understand the civilian CA model, why would they run poorly maintained CA with weaker security properties under a different brand name (RapidSSL), when they fully understood that this practice weakens the security of the global village? [PKI-022]

Clearly, if the wider public understood the significance of the serious weakness of the civilian CA model, or if there was an attack that was broadly felt by the public, then this would negatively impact on eCommerce and markets, and also the acceptance of eGovernment initiatives, because the guarantee of authenticity of certificates is critical in all these systems. [PKI-023]

John has read that the USA has used cyber attack against insurgents in Iraq (2003) and was also contemplating cyber attack against Iraq banks but stopped short of that due to the Iraq banks interconnectivity with banks in France²⁹.

John wonders what would happen if a Government forced a Root Certificate Authority (or Domain Name Authority ³⁰) to fake identities of a foreign country during a time of war? [PKI-024] What would happen if this escalated internationally?

John knows that issues like this have prompted President Obama to put cyber security to the top of his agenda, but these are international issues and John wonders what the EC is doing about them. Even though air transport is critical to tourism in the EU and therefore a high profile potential target for cyber attack, John doubts that there will be any mechanism or capacity to get these issues seriously addressed in the SESARJU project.

John knows that he does not need to look at the worst case ‘cyber war’ scenario. Cyber crime is already a very serious and growing problem which now has an annual global “turnover” in the criminal world of more than 1000 Billion USD [recent numbers from an FBI white paper] with the hardest hit industries being the banks and the insurance companies ³¹.

Approximately 86% of fraud happens by management at a level that can be *sustained by the system without reaching a level that causes sufficient attention* to expose the crime.

According to KPMG, U.S. companies lose an estimated **5 percent of their annual revenues to fraud** – about \$638 billion in 2006 alone, according to research by the Association of Certified Fraud Examiners ³². In a study of 360 fraud investigations conducted by KPMG in 2007, **89 percent** of the perpetrators committed fraud against their own organizations. **Based on actual cases** in Europe, the Middle East, and Africa, KPMG found that 86 percent of perpetrators in the cases studied held management positions; **60 percent of those were members of senior management or board members; 11 percent were chief executive officers (CEO).** [PKI-024]

What if identity fraud attacks were perpetrated by an organised a combination of senior management in banking and senior technical management in a certificate authority to misappropriate money in an international scheme? [PKI-025]

As John has thought repeatedly, PKI is a brittle system with many system-wide single points of potential trust failure. The most obvious line of approach to addressing the single-point-of-trust failure problem is to introduce redundancy

²⁸ <http://www.mail-archive.com/cryptography@wasabisystems.com/msg02344.html>

²⁹ Harris, S. *The cyberwar plan*. In National Journal Magazine (November 2009), NationalJournal.com. Available at http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php.

³⁰ O’Connor, T. *Week 3: International cyber crime and security, cybercrime and cybercriminals*. In Network security syllabus (December 2009). Available at <http://www.apsu.edu/oconnort/3100/3100lect02b.htm>

³¹ Oak Ridge National Laboratory, Cyber Security and Information Intelligence Research Workshop, <http://www.csiir.ornl.gov/csiirw>

³² KPMG. *Profile of a fraudster survey 2007*. Forensic advisory, KPMG International, April 2007. Available at [http://www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey\(web\).pdf](http://www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey(web).pdf)

into the system, such that trust around an identity is distributed amongst competing service providers – ensuring each identity was validated by two independent Root Certificate Authorities in some well-defined standardised way.

As a hardened pragmatist John knows that this could be an unpopular proposal in the established public key infrastructure industry that makes a lot of money out of the current model. John expects that even the industry generally would not agree to consider undertaking a new risk/cost/benefit analysis without clear support from Government. John expects that, without such an analysis, even an evolutionary upgrade would meet with industry resistance: [PKI-026]

- Root Certificate service providers could feign offence at the suggestion that their security systems were insecure or required the support of other root (sovereign) certificate authorities, as this might weaken their customers perception of the value of their existing service;
- Root Certificate service providers could argue that the (some consider exorbitant) costs they charge already for a 12 month certificate would have to increase further to support the extra effort needed to distribute trust and create resilience through redundancy creation across, and co-operation between, providers;
- Developers who are having trouble supporting the already complex public key infrastructure would have to retroactively upgrade every application to support dual standards;
- Customers ordering certificates might have to co-ordinate the activities of two recalcitrant certificate authorities;
- Not to mention internal objections from some senior management who currently had the opportunity to exploit their position as a single point of potential system failure or fraud; introducing a new system that distributed trust and created redundancy might expose existing fraud as much as remove the opportunities for fraud.

In the face of potentially entrenched self interest and arguments about added cost, and in the complete absence of a proper risk/cost/benefit analysis, John knows that an EC level, ‘whole of Europe’ comprehensive study needs to be done, coherently taking all the factors into account, aligned to the welfare of the global community and not just the interests of any one commercial/national organisation, industry or pressure group. [PKI-027]

John knows he is not alone in worrying about “*the identity management issue*”, however much of the conversation is discussed behind closed doors due to vested interests and different perspectives and agendas on the issue. Depending on who John talks to, the problem varies from one of protecting against technical weakness, to ensure smooth operation of the Internal Market, empowering citizens to control their own identity, enabling citizens to interact more effectively with Government, all the way to the extreme objectives of “*locking down*” the civilian population so they can track all their activities for law-enforcement purposes, and the militarisation of the Internet.

John has no idea how he might even begin to approach these issues in the SESARJU project, and rally the support of his management, much less how his managers might win the interest and support of the project ‘investors’.

John’s mind moves to consider the rapidly advancing US Cybersecurity Initiatives.

John is aware that the last near-term action point on the US 60-day Cyberspace Policy Review report is to “*Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation*”. [PKI-028]

US 60-day Cyberspace Policy Review report also states “*The United States must work actively with countries around the world to make the digital infrastructure a trusted, safe, and secure place that enables prosperity for all nations*”.

John is aware that subsequent to the publication of that Report, the US NIST held an official Cryptographic Key Management (CKM) workshop to³³: “*improve the overall key management strategies used by the public and private sectors in order to enhance the usability of cryptographic technology, provide scalability across cryptographic technologies, and support a global cryptographic key management infrastructure*”.

However John had wished these publications went further, to explicitly state that these designs must take into account the legitimate interest of *all* stake holders, and explicitly require that the design must mitigate against Militarisation, against designs that favour the “*National Interests*” of one Nation over all others, against the potential for “*fraud*” by certificate authority insiders, managing the system, and against the risk of targeted action against specific citizens or even cyber war that could be performed by instructions of (current or future) Governments.

³³ http://csrc.nist.gov/groups/ST/key_mgmt/

John is aware that there are calls emanating from inside NIST for “*resilience against quantum computing attacks*”, “*cost-effective, fault-tolerant, and highly available*”, and “*that in the light of quantum computing CKM system designers MUST look at means other than using public key-based key management systems.*” [PKE-002]

But as far as John knew, such a widely accepted identity/key management system does not exist yet. [PKE-006] He knows that the research into quantum cryptography is still in its infancy with a new attack brought in 2009^{34 35}. [QKD-001] Even so, its advocates state publicly that existing quantum key distribution systems are not suitable to protect the Internet. [QKD-002] This only leaves symmetric key technologies (the opposite of public key technologies) as the most trustworthy approach.

Like most security experts John knows that the US Navy is setting up a new Cyber Command at Fort Meade³⁶ (Headquarters of the US NSA) and that President Obama has sought a Budget approval of **3.6 billion USD** for the US Comprehensive National Cybersecurity Initiative (CNCI) for 2011 alone³⁷. [CYBER-002]

Apparently the US Army wanted “*to be in charge of security for the 11 million Internet users, seven million PCs and 15,000 networks belonging to the Department of Defense (which is the largest Internet user on the planet). All the services are scrambling to get their Cyber War defenses strengthened, but the air force wanted to be in charge.*” ... “*The U.S. Air Force is still advocating more Cyber War attacks by American Cyber War organizations.*”³⁸ See also³⁹

But as Mike McConnell, the Senior Vice President of Booz Allen Hamilton and a former Director of US National Intelligence stated in his Keynote Speech at the NIST CKM Workshop, “*the Cybersecurity Initiative is primarily to protect .mil and .gov information. Somebody should worry about .com. Ninety eight percent (98%) of the world is .com or .edu or .org or a foreign segment of the global internet.*”⁴⁰ [CYBER-004]

John wonders what the cost will be to support the necessary research and development, and globally coordinated efforts for that remaining 98%, and what role Governments, United Nations, and the Organisation for Economic Co-operation and Development will play [CYBER-005] and how the entrenched security organisations will move forward particularly if they is no clearly identified buyer in these harsh economic times.

In the civilian and EU sectors, John is aware of the massive momentum built up around the deployment of the 20th century security solutions using PKI, which he knows already protects transactions worth trillions and investments worth tens of billions. In spite of the latest cybersecurity risk analysis activities in the USA, and the identified and known risks to PKI, John knows that PKI is the main contender to protect all the latest European Government ICT initiatives and major infrastructure projects such as SESARJU. [PKI-029]

He knows that PKI is the main interoperable solution in most security vendors arsenal. It could be economic market suicide for any PKI vendor to advertise that their own products are at high risk of security failure due to multiple single points of potential failure and the advance of quantum computers. This industry stance is evident from the minimal corrective actions taken after the MD5 Rogue Certificate Authority attack. Vendors will rarely seek to point out the

³⁴ Makarov, V., Anisimov, A., and Sauge, S. *Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by eve*. In arXiv.org quant-ph (March 2009). Available at <http://arxiv.org/abs/0809.3408v2>

³⁵ Gerhardt, I., and Makarov, V. *How we eavesdropped 100% of a quantum cryptographic key*. In Hacking At Random (Har2009.org) (August 2009). Lecture video available at <https://har2009.org/program/events/168.en.html>.

³⁶ Gates, R. M. *Establishment of a subordinate unified U.S. cyber command under U.S. strategic command for military cyberspace operations*. Department of Defense memorandum, June 2009. Available at <http://publicintelligence.net/?p=1010>

³⁷ Chabrow, E. *CNCI budget request set at \$3.6 billion*. In www.govinfosecurity.com (February 2010), GovInfoSecurity.com an ISMG Corp. media property. Available at http://www.govinfosecurity.com/articles.php?art_id=2151&rf=020210eg

³⁸ Strategy Page. *The U.S. Navy Cyber Warriors Step Up*. In StrategyPage.com (October 2009). Available at <http://www.strategypage.com/htmw/htiw/articles/20091006.aspx>

³⁹ O’Connor, F. *Political cyberattacks to militarize the web*. In PC World - Business Center (March 2009), IDG News Service. http://www.pcworld.com/businesscenter/article/161142/political_cyberattacks_to_militarize_the_web.html

⁴⁰ Barker, E., Branstad, D., Chokhani, S., and Smid, M. *Cryptographic key management workshop summary (draft)*. Interagency Report 7609, National Institute of Standards and Technology, June 2009. Available at <http://csrc.nist.gov/publications/nistir/ir7609/nistir-7609.pdf>

almost total lack of resilience and distributed trust, or the major problems, faced by all organisations, with public key management. John knows they will not wish to point to the fact that, while PKI can reach to service millions of users, the US NIST has already published in the CKM Workshop Report that new solutions must be found that will allow it to scale several magnitude more in the near future. [PKI-030]

John however was working in the EU and he believed that the USA led the security agenda and that much of the US cybersecurity activity was largely unknown to his associates in Europe. There was new legislation being rapidly advanced in the USA that would require the US NIST to lead the USA's international cybersecurity standards initiative⁴¹ [CYBER-006], but John was unaware of an equivalent high level co-ordinated (or equivalently funded) response in Europe.

John was also aware of the need to protect individuals against erosion of liberty due to National Authority's being single points of control over their citizens participation in international systems. This dependency could be exploited to coerce other nations (for example if one nation through certain proprietary banking activity had access to much of another nations banking data), or to create cyber war against the globe, or could be used as a tool by an authoritarian power or Government against its citizens. [SPOTF-001] [SPOT-002]

John, like many security experts, was aware of this range of risks and threats but knew that due to the economic climate and entrenched interests, most security vendors would not be willing to allocate funds to the study and trial of new designs. [PKI-031] Rather they would want to maximise sales of their existing solutions, even though the UN Telecommunications Chief has publicly warned of the risk of the next world war being in cyberspace where there are no superpowers, because every citizen can be a super power⁴².

In short, John recognised that the magnitude of the issues is beyond the study and reach of any player, even a leading nation. It will be difficult for countries to make the necessary changes, for a globally appropriate system, when national self-interest is in play, and particularly for those countries militarising their cyber interests.

To provide one recent example of this type of governance difficulty, according to Peter Eigen (previously a director of the World Bank in Nairobi): *“In Germany there is a system where you are not allowed to bribe a civil servant, but you are allowed to bribe a deputy. This is under German Law allowed. And the members of our parliament don't want to change it. And this is why they cannot sign the U.N. Convention against Foreign bribery. One of the very few countries that is preaching honesty and good governance everywhere in the world, but are not able to ratify the convention.”* (2009).⁴³

John agrees with the President of the USA when he stated publicly recently, an international effort is required to create new cybersecurity standards. **But, in the absence of the highest level of leadership in Europe (and other regions), without a system of checks and balances, global identity management issues may not be addressed in a way that is appropriate to the European or global civilian community. With the militarisation of the Internet by foreign Governments, many of the “new standards” may become weapons of coercion and not tools of global social empowerment for the other 98% of the world's population.** [CYBER-007]

So right now, John has to focus on how we will manage this complexity with regard to the services and advice he will deliver to the security group which carries responsibility for a small but important part of the €2.1 billion SESARJU development phase. He knows that he took the simplest and most expedient path when he agreed to have his biometrics recorded and archived for his new passport and UK NIC, in spite of his own real and justified concerns and fears. John asks himself how he can morally argue that SESARJU should address these problems when he himself has subscribed to the system by choice driven by expediency. He knows that the major security vendors will probably be driven by prevailing economic conditions to promote existing certified solutions, rather than try with a limited budget to address the real issues and risks that apply to an international 30+ year project. Given the complexity and international scope of the risks and issues, is it even reasonable to expect that one project should try?

⁴¹ Lipinski, D. H.r. 4061: Cybersecurity enhancement act of 2009. Available at <http://www.govtrack.us/congress/bill/xpd?bill=h111-4061>.

⁴² Walker, G. ITU chief stresses need for cooperation to protect cyberspace. In United Nations Radio (October 2009). Article available at <http://www.unmultimedia.org/radio/english/detail/83203.html>, audio: <http://downloads.unmultimedia.org/radio/en/ltf/mp3/2009/n-itucyberspace.mp3?save> and <http://downloads.unmultimedia.org/radio/en/ltf/mp3/2009/n-toure2.mp3?save>.

⁴³ http://www.ted.com/talks/peter_eigen_how_to_expose_the_corrupt.html (13 minutes into talk).

5.2 Scenario: 2015 (Future Risks)

John is sitting nervously at the Heathrow Airport, waiting to board his plane (an impressive Boeing 747-8⁴⁴). With the international financial markets still recoiling from the second round of property mortgage write downs in the United States⁴⁵, the airport remains busy, however one imagines that there used to be more tourists at this time of year.

John is on his third espresso for the morning and distressed about the series of technical and political problems emerging against his SESARJU project. He was still in shock at how quickly these issues had moved from the background to become active threats.

John did win the job at Thales in 2010 and has been travelling internationally between the countries participating in the SESARJU and FAA NextGen Project to work on the identity management and cryptographic security aspects of the project.

His team had been assigned to work on P14.2.2⁴⁶ which was tasked to ensure that the System-Wide Information Management component of the SESARJU project was safe and secure. John and the other security experts had recently signed off a security standard based on US NIST public key cryptography. It was the available compromise option under the existing circumstances, acceptable as long as the SESARJU security parameters were limited to allow single points of potential failure, to allow a lack of resilience and redundancy and distributed trust, and to require only cryptographic security against classical attacks, and not security against known quantum computing threats. After accepting these parameters, it was relatively easy and affordable for John's P14.2.2 project to reapply vendors popular 20th century solutions. A predictably short sighted approach that, like the lack of security in the first deployment of the Internet [CYBER-009], was now starting to become painful [CYBER-008].

In his initial after-hour meetings with his new peers, John had raised the risks surrounding PKI. Some of his peers frowned, and the team leader politely advised John that “*of course*” it was only possible to use already accepted standards and that he would receive no support from his team if he raised it. [PKI-011]

John asks him self rhetorically what more could he have done?

John already knew, when started on the project in 2010, about the 2009 US NIST call for new solutions that were resilient against quantum computers and that did not rely on PKI. Now he is concerned that their new PKI based security architecture, targeted as it is to a 30+ year critical infrastructure project [PKI-003], might not see the light of day. If it does get deployed, John's stress levels will not diminish. He wonders how long it will be before the entire system may well need to be radically reworked, perhaps in a very costly rip and replace scenario. John is very aware that the old approach of trying to upgrade and add security on later was a losing game. *But he felt that he had been railroaded* by circumstances since 2010, and in particular he needed to keep his employment. John recalls that, like his colleagues, he had come to the conclusion that it was not possible to tackle the international issues of critical single points of control and potential failure, and they had rationalised that maybe large quantum computers would never come.

Taking another sip of his coffee, John recalled that the topic of quantum computers somehow never really emerged in any of the project discussions. There was he felt an institutionalised blindness on this subject and some vague expectation that quantum cryptography may evolve to one day provide the security solution to the quantum computing threats. [PKI-033] The SESARJU security team had taken the ‘*safest*’ approach and applied the current US NSA Suite B standards to the letter, which included PKI.

But 2 months ago, the problems had started.

⁴⁴ <http://www.boeing.com/commercial/747family/>

⁴⁵ Big Banks in Trouble: Huge Mortgage Write-Downs Seem Inevitable, http://seekingalpha.com/article/144554-big-banks-in-trouble-huge-mortgage-write-downs-seem-inevitable?source=article_sb_popular

⁴⁶ <http://www.sesarju.eu/programme/workpackages/wp-14-swim-technical-architecture--201>

At that time ECRYPT III (European Network of Excellence for Cryptology⁴⁷) published their Yearly Report on Algorithms and Key Lengths (2015). It was the first time it has been significantly revised since it had started in 2004⁴⁸. In all ECRYPT key-length Reports up until this one, the 12+ authors had side-stepped the issue of future computing capabilities with a disclaimer buried deep in the text around page 24 of the 71 page document: [PKI-034]

“The recommendations in this report assumes (large) quantum computers do not become a reality in the near future.”

In this revision of the ECRYPT Report, which was uncharacteristically 6 months late, the text was effectively rewritten to elevate the threat of quantum computer attacks to become a mid term risk that must be addressed in the immediate future. The paper reports that a joint effort between the US Quantum Information Program⁴⁹ at NIST and the EU Future and Emerging Technologies (FET) Proactive Initiative in Quantum Information Processing and Communication⁵⁰ had made a significant advance in ion-trap based quantum computation.

The unofficial word on the grape-vine is that the quantum information processing community advised certain cryptographic security advisors of the full significance of their discoveries behind closed doors, to permit them some time to search for a coherent strategy to recommend to their respective communities. The quantum information processing group advised that while the remaining steps are rather expensive, and will require a good number of person-hours, the remaining technical barriers appear to be surmountable. Furthermore, in light of the code breaking capabilities and also other benefits offered by large quantum computers, they advise that they have received priority “defence” funding to proceed. ECRYPT didn’t put a time frame on when they would arrive, however experts like Professor Seth Lloyd of MIT, who co-invented the world’s first (public) quantum computer in 1996, had never been afraid to make a prediction. In 2008 he had estimated code breaking computers could arrive after 2018. Professor Lloyd now publicly advised that, based on his information, code-breaking quantum computers may arrive after 5 years⁵¹ and that it is possible China could already be some way ahead. John wonders if maybe the breakthrough was made by, and then subsequently gleaned from, the Chinese?

John has now read the ECRYPT Report twice. It is well thought out and full of carefully worded disclaimers. It brought no joy to John. The ECRYPT Report advised that the international cryptographic community had made no focussed effort to evaluate candidate “post quantum secure” public key cryptography [PKI-036]. The very first conference focusing on the problem was held in 2006, then only every two years up until 2014. The progress was slow and there simply was not enough publications available nor sufficient interest to run the conference every year. Even as late as 2012 well over 90% of the papers on public key cryptography published on EPRINT⁵² were still based on constructions that could be attacked by code-breaking quantum computers.

ECRYPT advised in this Report that it can take up to 10 years of intense international study for the community to identify, test and hopefully accept a new quantum resilient public key algorithm, providing of course that one can be identified that can also survive the new quantum algorithms discovered over that period. This time projection is based on solid experience learned in other cryptography contests, for example the recent US NIST SHA-3 hash function competition had taken approximately 7 years to develop and gain consensus about a selected candidate in the international cryptographic community. The NIST hash function competition was a simpler process in that it was looking for stronger ways to randomly mix data together. Developing any new public key algorithm requires identifying new mathematical equations with very particular algebraic properties. Even without the added complexity of achieving resilience against quantum computers, these particular properties unfortunately already increase the difficulty in achieving assurance that there isn’t some ‘simple solution’ to breaking them. This problem was experienced with the classically secure ECC algorithm, which though being significantly more efficient, has taken years

⁴⁷ <http://www.ecrypt.eu.org/>

⁴⁸ Gehrman, C., Naslund, M., Babbage, S., Catalano, D., Granboulan, L., Lenstra, A., Paar, C., Pelzl, J., Pornin, T., Preneel, B., Robshaw, M., Rupp, A., Smart, N., and Ward, M. Ecrypt yearly report on algorithms and key sizes (2004). Deliverable D.SPA.10, IST-2002-507932 European Network of Excellence in Cryptology (ECRYPT), March 2005. Available at <http://www.ecrypt.eu.org/ecrypt1/documents/D.SPA.10-1.0.pdf>.

⁴⁹ <http://qubit.nist.gov/>

⁵⁰ http://cordis.europa.eu/fp7/ict/fet-proactive/qift_en.html

⁵¹ Lloyd, S. *Riding d-wave*. In Technology published by MIT Review (May 2008). Available at <http://www.signallake.com/innovation/RidingD-Wave042408.pdf>. Quote: "At current rates of progress, big, code-breaking quantum computers are at least a decade away."

⁵² Cryptology ePrint Archive, IACR. Available at <http://eprint.iacr.org/>

to win acceptance and only recently has begun to be deployed widely in the community. [PKI-035] The US Government was spending large sums to deploy ECC particularly for applications with its allies but it was an already well established fact that the ECC algorithm, like all other existing deployed public key algorithms, completely failed to code breaking quantum computer attacks. Unlike most systems, the US cleverly left themselves an insurance policy – ALL the US security modules replacing legacy systems in the field were required to support remote programming, so they could upgrade their field deployed security technologies.

One of the problems ECRYPT highlighted was that insufficient experts in the cryptographic community had taken the Government and privately funded research into code-breaking quantum computers seriously. It was also very unpopular to go around saying “*the systems we have will break*” when it was obvious to the community that there was no public key alternative available for the “*prime-time*” ready to promote. Entrenched interests ruled the waves and the dominant need to satisfy harsh economic realities had prevented a strong focus in the study of quantum resilient public key algorithms. Proposing new public key algorithms was also not very popular among cryptographers, as many attempts before hand been broken, and the chances of their proposals failing was also high.

The ECRYPT Report listed a handful of existing candidates, and advised that the EU had funded them to organise a 3 year fast-track program of testing to select the best public key candidate. [PKE-007] [PKE-008] Worse still, most cryptographers did not understand the full range of computing capabilities expected from quantum computers, and so could not evaluate the potential risks for the next generation public key candidates. [PKE-009] The US NIST made a different decision. The 2004 US ARDA Report had advised that new quantum algorithms would continue to be discovered, and that some of these could be expected to be relevant to the existing hard problems candidate public key algorithms are based on. That Report pointed to the theoretical existence of hard problems (random permutations) that were resilient to quantum computing era. The US already had one symmetric encryption (shared-key) algorithm that was conjectured to be secure under this model (AES-256). Furthermore the US and NIST were heavily invested into Quantum Key Distribution (Quantum Cryptography), a special type of symmetric (shared-key) cryptography. Of course a different division of NIST also performs advanced quantum computing research, and so results internal to NIST may have advised them of future risks. Therefore the NIST continued and escalated their 2009 call for designers to develop new symmetric key capabilities that did not rely on public keys. The global security community was now split. [PKE-002]

Free to use proposals supporting key distribution using symmetric systems in a way that employed multiple servers and distributed trust was proposed⁵³ in 1976 by the co-inventors of public key cryptography before the arrival of public key cryptography! This technology could have been adapted to build international key distribution systems of modest scale.

John was personally aware of proposals since 2007, based on the techniques in the 1976 proposal, that could enable a shift away from public key encryption for key distribution even in very large scale international systems. This could be achieved using just the AES-256, or AES-256 in combination with quantum key distribution (QKD) networks. NIST researchers clearly continue to receive funds to create advanced QKD systems, however NIST does not have to rely exclusively on this research to create a classically and quantum secure key distribution replacement. NIST can design new Cryptographic Key Management Solutions that use both techniques when available in a redundant manner, and fall back to use just AES-256 for Internet applications. Of course the dual model first required the discovery of a robust implementation of QKD, a solution that was free from attacks against the QKD implementation.

This shift away from public key encryption for key distribution can be achieved using just AES-256 for key distribution, or AES-256 in combination with QKD networks for key distribution. NIST researchers are clearly continuing to be funded to advanced quantum key distribution, however NIST does not have to rely exclusively on this research to create a classically and quantum secure key distribution replacement. NIST can design new Cryptographic Key Management Solutions that use both techniques when available, and fall back to just AES-256 otherwise. This way if a robust manner of implementing QKD was finally discovered, a solution was free from attacks against the implementation, the NIST research could be rapidly integrated by the CKM solution they designed and was already in production use in parts of the globe.

However, like the majority of cryptographers at the time, John was on a team that felt it had no option but to adopt the existing Government standards based public key cryptography. After all, it was what he knew from his earlier work in TSCP, it was what the US and EU Governments were using at the time, and it was the politically safe decision.

⁵³ Diffie, W., and Hellman, M. E. Multiuser cryptographic techniques. In AFIPS '76: Proceedings of the June 7-10, 1976, national computer conference and exposition (New York, NY, USA, June 1976), ACM, pp. 109–112. Available at <http://doi.acm.org/10.1145/1499799.1499815>. Available at: <http://portal.acm.org/citation.cfm?id=1499815>

But now PKI was a political land mine...

Last month, the Transport Committee urgently rushed an agenda item on to the European Parliament agenda to exchange views on the security of SESAR against quantum computer attacks over its 30+ year operational life span. The primary focus of this agenda item was, “what defensive actions would be taken by SESAR” and most importantly “what would it cost”. Once again, the failure to build in long term security from the outset had committed the SESAR project to the old cycle of trying to add in the necessary security later!



Patrick Ky, Executive Director of SESAR (illustrated as the speaker to the right⁵⁴), said this was the first time he had personally heard of this risk. Like others big projects being called to account, Patrick asked for time so that he could organise a comprehensive report to be compiled that could be understood by himself and the members of Parliament.

John took another sip of his coffee.

John knew that he, his team, and the organisations they worked for, would probably be able to side-step responsibility for the problem. [PKILS-001] This potentially catastrophic problem effected every standards based security system on the planet, and his organisation wasn't the only one under the gun.

The issue his team faced now was the same issue that they could have begun to address at the beginning of the project, but hadn't. They were now under pressure to seriously begin looking for a cost-effective and rapid solution. The purpose of the meetings in the USA was not to identify who was accountable, but to evaluate the different recommendations of ECRYPT and the US NIST, and to search for a suitable solution. However, the team was having difficulty defining “suitable”. Suitable cryptographically, financially or politically?

In critical infrastructure projects the development process is undertaken at more rigorous levels. Comprehensive risk models are developed and studied.

In spite of certain levels of risk management process, the US cybersecurity initiatives had conclusively established that this is not the case for cryptography. Certain assumptions and practices are simply carried forwards from the past. Brian Snow was Senior Technical Director of the Information Assurance Directorate of the US NSA. Snow is on public record since 1999 stating that we need assurances in the civilian security industry⁵⁵. Speaking at international conferences around the World, Snow stated in 2005:

“The software security industry today is at about the same stage as the automobile industry in 1930; it provides performance but offers little safety, and that is the security industry.”

“Looks nice, goes fast, but in an accident, you die!”

Now John and his team needed to look carefully at the symmetric solution approach being advocated by the USA. There are significant structural differences between a public key cryptosystem to a symmetric key solution. The cost of now rigorously developing either approach would be about the same. However, at this late stage in the project, the shift from public key to symmetric key would be effectively the same as restarting the analysis in this aerospace application from scratch. This would be politically very unpopular.



⁵⁴ Image courtesy – <http://www.sesarju.eu/news-press/news/hearing-sesar-european-parliament--488>

⁵⁵ Snow, B. *We need assurance*. In Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems (January 1999), vol. 1717 of Lecture Notes In Computer Science, Springer Berlin / Heidelberg Springer Berlin / Heidelberg, p. 725. Available at <http://www.springerlink.com/content/33qe0m8c8ahlthmr/>.

If his team adopted the NIST “symmetric key approach” at this late time, it would mean that most of the work based on “public key technologies” completed since 2010 would effectively be discarded and could not be significantly reused. John knew that this was a predictable problem that now faces every EU funded security project. John didn’t want to think about how low the return on investment for projects that continued to press ahead with at risk public key cryptography when they could have used robust alternatives.

Given the known difficulties with, and risk of not, actually discovering a trustworthy public key solution that might be resilient against quantum computers, John expected that ultimately the US preference for symmetric based solutions would take precedence over Europe’s preferred path. However right now there were urgent time-line pressures.

John knew that with the tight financial economic times they were in, and with such a late correction in the development process, schedules might be delayed, and the immediate and short term costs could be significant. However, if the system is not secure in practice, you may as well not have put in any security mechanisms in the first place.

John was torn between the two choices: Commit to using experimental next generation public key cryptography based on the pending 3 year EU competition [PKILS-001] and reuse the teams existing work and ignore the single point of trust failure issues, or rework the solution to use the more conservative symmetric key solution with its higher up-front costs at this time in the development life cycle. He didn’t like either choice under the current political circumstances.

John receives a one-line SMS on his iPhone from one of his international colleagues.

It reads “*Visit Cryptome before you arrive and be ready.*”

John turns on his second Generation Apple iPad and opens up the page to Cryptome, the security and Government watchdog site⁵⁶. John can’t find any new articles on quantum computing, but finds a prominent new link regarding the US Federal PKI Bridge.

John taps on the link and begins to read the page.

Apparently one of the many servers in the US Federal PKI Bridge system (as currently used by the aerospace sector) was hacked from a computer in America that was controlled remotely from a computer in China. [PKI-020] Apparently the electronic identity of a highly skilled contractor working on a military jet navigation system was hijacked, as was the identity of the system administrator for that project by breaking this one node. Together the two identities were used to capture the intellectual property of the navigation system, and then to add insult to injury, the data was deleted from the US servers. To make things worse, the attacker was able to also delete the online remote backup server which was physically located in a building in a different state. In this project, apparently there were no “offline” backups because they felt remote site online mirroring was previously assessed to be sufficiently secure, because the risks in the current identity management system were not accurately taken into account.

While the attack appeared to come out of computer run in China, and there is a history of such attacks [http://www.militaryphotos.net/forums/showthread.php?172973-The-top-10-Chinese-cyber-attacks-\(that-we-know-of\)](http://www.militaryphotos.net/forums/showthread.php?172973-The-top-10-Chinese-cyber-attacks-(that-we-know-of)) there are some pundits arguing that maybe the computer in China was also remotely controlled, this time by a small, politically motivated cyber-terror group interested in increasing trade difficulties between China and the United States for their own advantage. China was also refusing to co-operate with US investigations because of posturing with regard to international cyber-security policies.

Unlike the Rogue Certificate Authority Attack which broke the hash function used in the certificates to exploit a single point of trust failure in the certificate authority system, this attack did not break any crypto. Instead, the attacker exploited a buffer overflow problem in the operating system of a computer that had software that talked with a network attached hardware security module to sign identity certificates. The attacker was able to remotely gain access to the computer, and then by pretending to be the authorised software, forged a request to the hardware security module managing the private keys of the certificate authority to sign new identities on behalf of the attacker.

Just like the Rogue Certificate Authority Attack, the attacker exploited the system-wide single point of trust failures in the US Federal PKI, Certipath, TSCP security model to attack other users. [PKI-020]

John stares blankly at the ground, wondering how he can side-step addressing this latest issue in his next meeting...

⁵⁶ <http://www.cryptome.org/>



“Given their power to intercept and disrupt secret communications, it is not surprising that quantum computers have the attention of various U.S. government agencies. The *National Security Agency*, which supports research in quantum computing, candidly declares that given its interest in keeping U.S. government communications secure, it is loath to see quantum computers built. On the other hand, if they can be built, then it wants to have the first one.”

– Professor Seth Lloyd of MIT 2008
co-inventor of the first quantum computer [PKI-036]
(Image: http://www.edge.org/documents/life/life_index.html)

5.3 Scenario: 2019 (Known Future Risks)

John Smith is reclining in his seat in the business class of an Airbus A380-900⁵⁷, flying at an altitude of 30,000 feet, heading towards Los Angeles Airport. John is still working for Thales in security, but no longer on the SESARJU project. John is working on a new project.

After the second suite of mortgage write-downs that happened around 2014, there was increased pressure to independently audit the US Federal Reserve for the first time in its history. A revised version of the H.R. 1207 Federal Reserve Transparency Act of 2009⁵⁸ was signed into Law in 2016. The transparency, accountability and ‘independent audit’ trail fever flowed on to other unrelated industries, including the information technology security sectors. John had been called on to participate in an international expert panel to independently audit and sign-off on a highly technical but unclassified component of a large report on the “state of affairs” of the US Critical ICT Infrastructure.

John’s mind wanders back to the SESARJU and NextGen meetings of 2015. John recalls how these meetings were more political than technical. The technical options available were reasonably clear, the path forward was not. Slowly a strategy emerged. There were two options: (a) adopt the public key algorithm selected by the 3 year fast-track program to evaluate candidates when it became available or (b) rework the analysis to use symmetric key techniques. Both techniques would be ‘computationally secure’ in the short term. Option (a) would be cheap to adopt, and *might* be secure into the future. Option (b) would require reworking the security model at about the same cost as already incurred but would provided significantly higher assurance in the long-term. [PKI-037]

The security team did not want to be responsible if the public key algorithm selected under stress by the ECRYPT failed in the future, furthermore they didn’t want to be responsible for rocking the boat with the rework option this late into the project. The strategy that emerged in the security group was to shift the hard decision away from themselves towards upper management and investors in a way that they (and their security organisations) could later take advantage of, irrespective of the selection made by management. After all, if the public key algorithm failed, they could say that they offered the most cost conservative solution, but management did not listen to their warnings that the cheaper option of public key algorithm may fail. [PKILS-003]

With the help of the desktop publishing team, and a graphic artist, a short glossy report was prepared. The two options were presented side-by-side, with the positive and negative points listed side by side. Technical terms like “Computationally secure against *best known* attacks” were used to describe both options. The financial costs and timeline extensions were listed for both options.

The glossy short paper was indeed visually impressive, *appeared* comprehensible to the lay-man and was supplied to the administrative team. The paper was crafted so that cryptographers could later argue they accurately presented the risks, but they knew that executives and managerial staff would read both options as being adequately secure. Management and investors would immediately identify that the first option was far less costly, apparently less risky at at project execution level and it was clear to management and the investors that their liability might be shifted away from the project and towards ECRYPT if the new cipher turned out to be a dud. Also, it was politically expedient for the SESARJU project to rally behind ECRYPT. Of course ECRYPT had made the hard and unpleasant decision to rapidly find a replacement public key algorithm because they felt intense pressures from industry to find a low cost solution.

⁵⁷ http://en.wikipedia.org/wiki/Airbus_A380#Improved_A380-800

⁵⁸ <http://www.govtrack.us/congress/bill.xpd?bill=h111-1207>

Not surprisingly, the SESARJU project selected to replace the NIST approved ECC public key algorithm with the risky ECRYPT public key alternative. Furthermore, the single-point of trust failure was pushed aside again. In this way, 95% of the original work-effort was salvaged, at the expense of much lower assurances.

The fasten seat belt sign lights up and the plane begins to reduce altitude.

John’s gut clenches a little with the shift in pitch. As an air traffic consumer John had hoped that the very best long term security was being deployed to ensure the safety of his journey. After all, safe air travel was also essential for tourism in Europe. Today, John is not feeling safe during his flight. The original proposed minimum key lengths had to be increased due to advances in cryptanalysis against ECRYPT’s initial parameters on the new public key cipher they had selected, and John is among those who feel a general unease that maybe someone might see a fatal flaw that would be obvious in hindsight (e.g. when you rewrote the mathematical problem in another way). [PKE-008] John thinks of the all electronic cyber enabled ground-to-air forward trajectory planning that has been implemented to enable a lower noise, low power aircraft approach. John knows that more planes are flying on the same efficient flight trajectories because the flight plans are managed electronically. There is less margin for error now.

The safety of the flight depends in part on the security of the cryptographic algorithms. With the reduction in air-traffic management costs, there has been a direct reduction in the number of human controllers. If the system has to return to manual control with the 2x increased traffic density, there will be a much higher risk of a mistake in the intense confusion and density of incoming flights.

Worse, if during that time an attacker could alter the flight plans undetected by performing a man-in-the-middle relay attack, the chance of a collision increases significantly. The lack of distributed trust, redundancy and resilience in the PKI dependent air traffic control systems makes a catastrophic attack possible. John recalls the public prediction voiced by Mike McConnell, the Senior Vice President of Booz Allen Hamilton and a former Director of US National Intelligence that a catastrophic event will happen and that we will all be screaming. John is feeling decidedly queasy.

John’s plane lands safely.

John grabs his 9 year old biometric passport and proceeds to clear himself through customs.

John waits in queue to be processed by the “millimeter wave” scanner (illustrated to the right) that effectively performs a virtual strip search⁵⁹ to check for substances such as weapons, undeclared money and drugs^{60, 61}.

John follows the guidance of the Transportation Security Administration officer, moving his arms in ways to maximally expose his body to the 3 dimensional imaging system.



⁵⁹ Image to right and information from: <http://publicintelligence.net/scanner-porn/>

⁶⁰ Kodo Kawase, Yuichi Ogawa, Yuuki Watanabe. “Non-destructive terahertz imaging of illicit drugs using spectral fingerprints” Available at: http://www.riken.go.jp/lab-www/THz/71_k02.pdf

⁶¹ http://www.kwicksoft.com/html/millimeter_wave.html



John then proceeds to the “Rogue DNA 9000 eGate Automated Border Control Gates” illustrated to the left⁶².

The eGate instructs John to scan his passport, then his fingerprints and then look into the high resolution video camera so that facial and eye recognition can take place. John is instructed to show the front and side profiles of his face.

The process is completely automated without human intervention.

However, even with the central ICAO PKD in place, **John knows that this border control step is only as strong as the security of the public key cryptography.** If the private key of a country’s root certificate authority is recovered, the electronic data can be forged. The forgery could only be detected if the data being signed is checked against a remote database (there by completely undermining the purpose of public key crypto in the MTRD project).

With the advance of quantum computing progressing strongly, there is discussion of a large scale international recall of all ICAO e-Passports that use at risk public key cryptography. This is roughly estimated at well over 80% of all issued passports at this time. The whole ICAO MTRD scheme is up for redesign, with the US pushing for a system that does not rely on public key cryptography at all.

The insider security news is that a small quantum computer probably exists "somewhere". According to sources in the defence community there have been at least 3 detected security breaches of access control systems that cannot be otherwise explained. It appears systems that are relying on the modern NSA Suite B 256-bit or smaller Elliptic Curve public key algorithms may be subverted at will and if that is the case, then it won't be long before 512-bit ECC and 1024-bit RSA and D&H algorithms will also fall. [PKE-010]

| Classical security rating in bits | Factoring algorithm (RSA) | | | EC discrete logarithm GF(p) (ECC) | | |
|-----------------------------------|---------------------------|--------------------|------------------------------|-----------------------------------|-----------------------|------------------------------|
| | $\log_2(N)$ | \approx # qubits | \approx time | $\log_2(N)$ | \approx # qubits | \approx time |
| | | $2(\log_2 N)$ | $4((\log_2 N)^3)$ | | $\approx 6(\log_2 N)$ | $360((\log_2 N)^3)$ |
| 80 | 1024 | 2048 | 2^{32} | 163 | 1000 (1200) | $2^{30.5}$ |
| 112 | 2048 | 4096 | 2^{35} | 224 | 1300 (1600) | $2^{31.9}$ |
| 128 | 3072 | 6144 | $2^{36.7}$ | 256 | 1500 (1800) | $2^{32.4}$ |
| 256 | 15360 | 30720 | $2^{43.7}$ | 512 | 2800 (3600) | 2^{33} |

Table 1. Comparison of breaking RSA and EC using a quantum computer under equivalent classical security

As the table above illustrates^{63, 64}, code-breaking quantum computers easily solve the hardness of the mathematical problems that all Government standards public key crypto relies on. This cannot be fixed by increasing key lengths. Increasing the ECC key size from 163 to 512-bits results in a negligible increase in work difficulty. Simply speaking, these standards become useless and breakable in practice.

And it is this very issue that John and other experts have been called to advise on in an international expert panel.

⁶² <http://www.roguedna.com/egate.htm>

⁶³ Lov K. Grover, Jaikumar Radhakrishnan, “Quantum search for multiple items using parallel queries”, <http://front.math.ucdavis.edu/0407.4217>

⁶⁴ John Proos and Christof Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves", Quantum Information and Computation, 3 (2003), pp. 317-344. <http://citeseer.ist.psu.edu/proos03shors.html>

The technical but unclassified component of the report on the “state of affairs” of the US Critical Infrastructure that John is working on studies the implications of these attacks on sensitive data that has already been transmitted over these networks using these security technologies.

The problem is that all captured and archived “ciphertext” can be decrypted at will to expose the original messages. Nobody knows for certain how long the quantum computers have existed for, or how much sensitive data this attacker (or their network of associates) has access to. It can be reasonably assumed that many hackers will be discretely advertising their archived data, recorded in ‘wait-and-see’ attacks, and so now it is desperate scramble to try to prevent the quantum enabled attackers from systematically receiving all such data.

The first concern is that an attacker may be systematically exposing US classified data and intellectual property.

The second concern is that they may use this computer to create undetectable fake electronic identities and remotely access critical infrastructure systems to disrupt them.

One of the scenarios the U.S. is worried about is that a co-ordinated attack might simultaneously shut down the majority of power stations in the U.S and open up the dams... John wonders if this is what Mike McConnell, the Senior Vice President of Booz Allen Hamilton and a former Director of US National Intelligence was thinking in his Keynote Speech at the NIST CKM Workshop (2009) when he predicted *“that we're going to have a catastrophic event, and then we're going to be screaming.”*

John knows that if the existence of the quantum computer, and the vulnerability of most existing security systems and the conclusions of this report were leaked, it would undermine the security of both the US and EU internal markets.

END SCENARIO

6. Rationale / Significance of proposed scenario

6.1 Why study public key cryptography?

The growing number of security breaches has already generated substantial financial damage, has undermined user confidence and has been detrimental to the development of e-commerce. As early as 2002 many leading security experts wrote an open letter to President Bush⁶⁵ and advised that the US ICT infrastructure was at grave risk. Today their opinion is publicly confirmed.

To quote extracts from the 9 June 2009 Keynote Speech by Vice Admiral J. Mike McConnell (USN Ret)⁶⁶ at the USA NIST National **Cryptographic Key Management** (CKM) Workshop:

“The Internet has introduced a level of vulnerability that is unprecedented. ...

***The nation is at strategic risk.** ... I was in a group that had an opportunity to brief then-candidate Barack Obama on security on the 2nd of September 2008. ... **President Obama is now addressing cybersecurity at the most senior level.** The Cyberspace Policy Review that was just issued attests to that. However, the Cybersecurity Initiative is primarily to protect .mil and .gov information. **Somebody should worry about .com.** Ninety eight percent (98%) of the world is .com or .edu or .org or a foreign segment of the global internet. ...*

[CYBER-007]

***My prediction is that we're going to have a catastrophic event, and then we're going to be screaming.** We have an opportunity to address and solve Internet problems before we have that anticipated catastrophic event. **We now have the attention of the new President.** ...*

***We must design and build security into the new Internet.** We must include countries such as Russia and China in creating the design. **We have to do this because the globe could be so advantaged by this secure Internet capability and is currently so vulnerable.** Something big must be done now.”*



– Mike McConnell is a Senior Vice President of Booz Allen Hamilton and a former Director of US National Intelligence. He previously served as Director of the US National Security Agency. President Obama has asked McConnell to continue to serve on his President’s Intelligence Advisory Board (PIAB) which advises the President on all matters related to intelligence.

McConnel is stating that the status quo with regard to security is a risk that could undermine the smooth functioning of the Internal Market. McConnel is calling for action now to ensure that the integrity and security of public communications networks for 98% of the world is ensured. This 98% of the world includes Europe.

***Identity Management is an emerging focal point in both the EU and the US political agendas as a critical component of cyber security that must be improved.** [PKI-038]*

Identity Management and Cryptographic Key Management are tightly interrelated.

Public key cryptography is the dominant technology used in cryptographic key management and identity management today.

Public key cryptography and public key infrastructures are known to be at risk.

The RSA (Rivest-Shamir-Adleman) Algorithm is an example of the most popular Public Key Algorithm deployed in public key infrastructure. It already protects transactions worth trillions and investments worth tens of billions. The recent alternative to the RSA algorithm is another type of public key cryptography based on Elliptic Curves. Elliptic Curve Cryptography (ECC) is increasingly being used instead of RSA in new applications because it is more efficient.

⁶⁵ <http://www.uspcd.org/letter.html>

⁶⁶ Public domain image and wikipedia article on http://en.wikipedia.org/wiki/John_Michael_McConnell

Taken together the RSA and ECC public key algorithms, and the public key infrastructure that uses them, are employed in virtually all eCommerce and all eGovernment, in all eID schemes such as ePassports.

They are the dominant technology that is used TODAY to offer Identity and Key Management on the Internet. Both algorithms are vulnerable to code-breaking quantum computers.



Massive investments have been made into PKI, today the global society (including Europe) has a dependency entirely on PKI, and the dependency is growing with massive further PKI rollouts planned. [PKI-001] [PKI-029]

Examples of ongoing and planned rollouts:

- a) Fraunhofer, one of the largest research institutions in Europe is just now implementing its public key based eID;
- b) the UK government intends to link all UK Government departments using PKI (CIPHER Project);
- c) PKI will be used in major long term (30 + year) future critical infrastructure projects such as SESAR/NextGen;
- d) Galileo;
- e) EC requires biometrics by law in many areas e.g. biometric ePassports, nuclear power stations (biometric systems rely on PKI); and
- f) many more examples.

What are the risks associated with this massive global dependency on Government sponsored PKI?

- The US NIST has identified major risks with today's PKI [PKE-002] and says CKM must be part of the US and international cybersecurity initiatives (discussed in section 6.4.3.2);
- NIST has already launched a major CKM Project [PKI-005];
- the US Federal Government is now advancing new Laws that will authorise and require NIST to co-ordinate the USA's international cybersecurity collaboration to create new international cybersecurity standards [CYBER-006];
- The US NIST publishes "*We know how to handle (cryptographic) key management reasonably effectively for up to a million people, we need to go a couple of orders of magnitude beyond that in the relatively near future*" [PKI-030]

Risks identified by NIST and others:

The whole world is already gambling with global stability, and is continuing to do so in its next generation major projects, by depending on a global security system:

- that has no resilience or redundancy;
- that uses one algorithm and what if it breaks!!
- no separation of powers,
- does not distribute trust across separate powers,
- any one PKI authority can go rogue and disrupt the entire global system [PKI-021];
- quantum computers expected in 9+ years according to the United States Advanced Research and Development Activity⁶⁷ (ARDA) report⁶⁸ and other experts [PKE-003].

International trade and communications needs resilience and distributed trust to prevent single points of control and potential global failure, etc. These features are absent in the current PKI infrastructure.

Large organisations and government bodies require a >5 year duration of data security and may take more than a decade (such as EMVco) to upgrade their computing systems. These organisations require known catastrophic future risks to be comprehensively addressed in their production systems well before those risks could threaten the operation and survivability of that organisation, and to protect third party sensitive data they are entrusted to manage.

⁶⁷ <http://qist.lanl.gov/>

⁶⁸ Hughes, R., Doolen, G., Awschalom, D., Caves, C., Chapman, M., Clark, R., Cory, D., DiVincenzo, D., Ekert, A., Hammel, P. C., Kwiat, P., Lloyd, S., Milburn, G., Orlando, T., Steel, D., Vazirani, U., Whaley, B., and Wineland, D. A *Quantum Information Science and Technology Roadmap, Part 1: Quantum Computation, version 2.0*. Tech. rep., Advanced Research and Development Activity, 2004. Available at http://qist.lanl.gov/pdfs/qc_roadmap.pdf



“The next world war could taken place in cyberspace and this needs to be avoided. The conventional wars have shown us that first of all there is no winner in any war and second the best way to win a war is to avoid it in the first place. So we need to plant the seeds for a safer cyberspace together. It can only be done at a Global level because the criminal no longer needs to be on the crime scene and you can attack many places at the same time in cyberspace” ⁶⁹

“There is no such thing as a superpower in cyberspace, because every individual is one superpower in itself, because it is the human brain that makes a difference in this field. This is one natural resource that is equally distributed in the world.” ⁷⁰
[CYBER-001]

– Dr. Hamdoun Toure, UN Telecommunications agency chief, 6 October 2009
(Image from <http://www.unmultimedia.org/radio/english/detail/83203.html>)



“A decade into a new century, this old architecture is buckling under the weight of new threats. The world may no longer shudder at the prospect of war between two nuclear superpowers ... but modern technology allows a few small men with outsized rage to murder innocents on a horrific scale.”

-President Barack Obama, Nobel Peace Prize Ceremony, Oslo, 10 December 2009

“From now on, our digital infrastructure ... will be treated as a strategic national asset ... we will develop a new comprehensive strategy to secure America's information and communications networks.”

- President Barack Obama,

Remarks by the President on securing our nation’s cyber infrastructure, 29 May 2009

These issues all amount to being multiple single points of potential global catastrophic failure, pose risks to the European community in the broadest sense and to the individual citizen, and all business and the safe development of the Union; PKI with all these risks can be exploited to create cyber war where one party can hold the world to ransom, or one party can singled out as a target; and it IS impossible to reduce this global dependency on PKI overnight or to guarantee the long term safe operation of critical infrastructures programs and projects...

Therefore ENISA needs to recommend to the EC that it launch an urgent study on these risks, and how to protect against them...

This is a low risk step as some of these risks are now being openly discussed now in the US cybersecurity initiatives and in particular in the US NIST CKM Project.

“Recommendation 6:

The EC should recognise that, in order to be effective, it should address the global dimension and foster engagement in international discussions, as a matter of urgency, to promote the development of open standards and federated frameworks for cooperation in developing the global Information Society.”

– “Trust in the Information Society”

a report of the advisory board RISEPTIS in collaboration with Think-Trust.

“The United States must work actively with countries around the world to make the digital infrastructure a trusted, safe, and secure place that enables prosperity for all nations”.

– U.S. President’s Cyberspace Policy Review, 2009

⁶⁹ <http://downloads.unmultimedia.org/radio//en/ltd/mp3/2009/n-itucyberspace.mp3?save>

⁷⁰ <http://downloads.unmultimedia.org/radio//en/ltd/mp3/2009/n-toure2.mp3?save>

6.2 US is drafting new laws to give NIST authority to interact with international standards organisations

House panel OKs law addressing cyberstandards

Angela Moscaritolo

November 05 2009

A draft bill approved Wednesday by a House subcommittee **would require the National Institute of Standards and Technology (NIST) to facilitate U.S. involvement in the creation of international cybersecurity standards.**

The proposed *Cybersecurity Coordination and Awareness Act*, approved Wednesday by the House Subcommittee on Technology and Innovation, would also require NIST to develop and implement a cybersecurity awareness and education program and **engage in research and development to improve identity management systems.** Also, it would amend the *Cybersecurity Research and Development Act* to update technical terms.

The proposed legislation was **drafted by staff of the House Committee on Science and Technology to implement some of the recommendations in the 60-day Cyberspace Policy Review**, a report released this May that outlines the federal government's new approach to securing cyberspace. According to the review, **international standards are needed for the investigation and prosecution of cybercrime, the approaches for network defense and response to cyberattacks.**

"The Cyberspace Policy Review recommended coordination of U.S. government representation in international cybersecurity technical standards development," Subcommittee Chairman Rep. David Wu, D-Ore., said in his opening statement Wednesday. "Currently, responsibilities are parsed among different agencies without any consistent policy. A coordinated policy will ensure that these representatives operate with the overarching need of the U.S. infrastructure in mind."

The proposed legislation would require NIST to coordinate U.S. representation with regard to international cybersecurity standards development and create a plan to engage with international organizations to develop standards.

...

The proposed legislation now will move to the full House Committee on Science and Technology.

<http://www.scmagazineus.com/house-panel-oks-law-addressing-cyberstandards/article/157153/>

The above proposed legislation was then combined with a draft bill to address cybersecurity research and development and is now called the Cybersecurity Amendment Act of 2009. The combined draft rapidly passed the full House Committee on 4 Nov 2009. [CYBER-006]

<http://www.scmagazineus.com/house-committee-passes-cyber-rd-standards-bill/article/158110/>

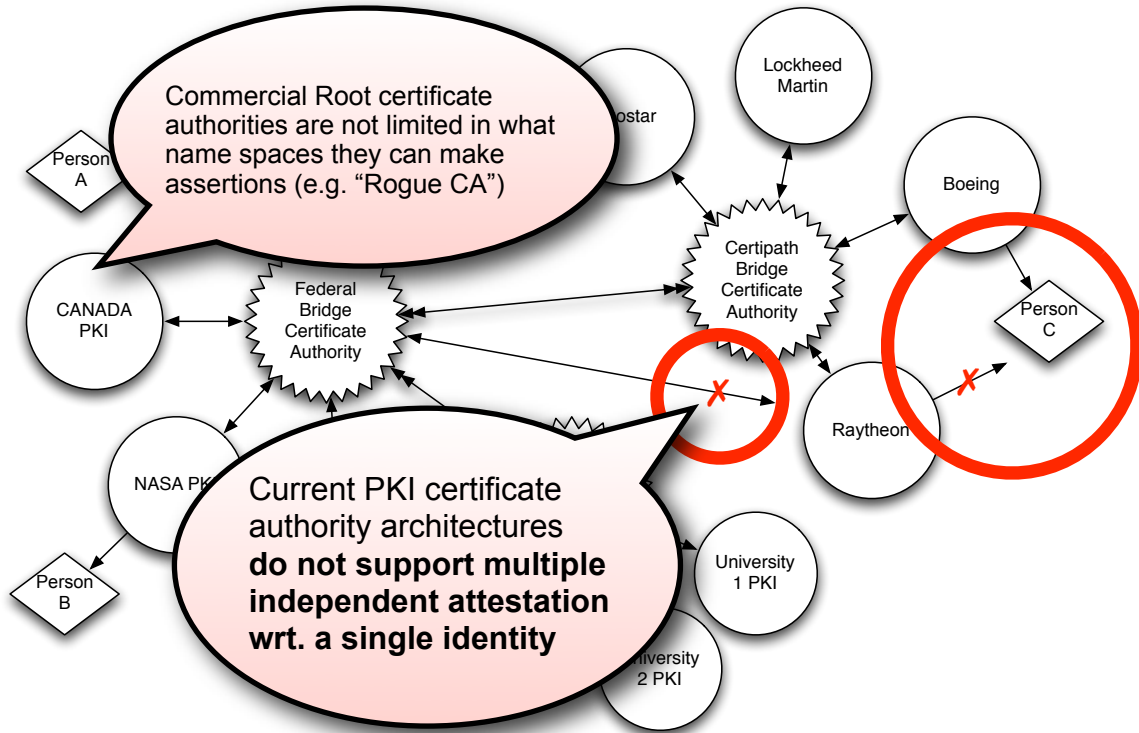
At the time of this publication H.R. 4061 has not yet been signed into law.

See this link to check its current legal status: <http://www.govtrack.us/congress/bill.xpd?bill=h111-4061>.

6.3 High level explanations of the technical problems found in the scenario and identifying future solutions

6.3.1 What does a single point of trust failure in ID systems look like?

Below we illustrate the US Federal PKI Bridge and its extension into international Aerospace and Defence organisations through the Certipath bridge.



In the illustration above Person C is attested to by Boeing. If person C is a contractor, Raytheon cannot attest to the same identifier created for Person C by Boeing. Raytheon needs to assign a new identifier to Person C. Because of the lack of redundancy in the attestation process, the identifier associated with person C by Boeing can be falsified to any organisation within the federated system if Boeing's Identity Management processes are compromised. [SPOTF-003]

This problem is most visible in the next section where we talk about the Rogue Certificate Authority Attack demonstrated at the beginning of 2009.

As an aside, we note that the identity assertions are not connected back to the authorities responsible for managing their respective name spaces. A PKI certificate for "John Smith" is not connected back to the Birth, Deaths and Marriage Registries of any nation. We have no way of validating that a "John Smith" born in London in 1950 is a real identity, and if that person is actually alive. In much the same way, if we receive a PKI certificate for a web server "MyBank.com" there is no way to validate that the certificate authority provider was permitted to make an assertion regarding "MyBank.com". We argue that it is not sufficient to validate a path back to a single root certificate authorities such as Verisign or Canada PKI. There must be multiple assertions, made from different authorities, regarding any given certificate.

The US Federal PKI bridge illustrated above to the left is an existing technology. The process of bridging through Certipath started "about 5 years ago by the MoD and the [UK Council for Electronic Business \(UKCeB\)](#). At the Outset the DoD joined together with a number of Aerospace and defence companies in Europe and the U.S. The objective was to solve a number of problems concerning security of information when undertaking collaborative activities between companies, governments and individuals in a post 9/11 world."

TSCP now promotes a new secure email standard that is based on the use of the Federal PKI Bridge and Certipath. The proposed new standard was completed in September 2007 and is now an emerging technology in the Aerospace and Defence community.

6.3.2 Costs associated with security failures of a single certificate authority

We quote the section “*Risks Associated with Certification Authorities*” on page 8 of the following letter⁷¹ by the United States Government Accountability Office:

Certification authorities, when used to bind agencies, their employees, and others contracting with agencies for financial management transactions, are a critical component of a PKI regardless of whether a federal or commercial entity operates the certification authority because of the importance that the certification authority has in the PKI trust model. [...] The certification authority is the entity that the other users of the PKI trust to guarantee the association between a public key and a specific user or entity. Accordingly, **if the certification authority is compromised the impacts can be catastrophic to an agency’s operations. [PKI-021]** This is especially true if the compromise is not immediately detected for some period of time since improper certificates could be issued to individuals or organizations that could be used to make improper payments for one or many improper transactions. [PKI-025]

Since all parties trust the certificates issued by the certification authority, an undetected compromise may, depending on what other controls are present, result in the systems that rely on those certificates making improper payments.

For example, a financial management system may rely on a contracting officer's certificate to ensure that an obligation is valid before entering it into its records. The financial management system may also rely on a certificate issued to another individual to validate that the goods and services associated with that contract have been received and accepted by the agency. Once the financial management system is notified that an invoice has been received for these goods and services, it may automatically generate a payment since (1) a valid obligation has been recorded, (2) the goods and services called for in the obligating document have been received and accepted, and (3) an invoice has been received. This is a classic automated three-way match that leading financial management systems perform to reduce the costs associated with payment processing.

Simply stated, because of the trust the system places in the certificates issued by the certification authority, the system may securely transmit an improper payment based on the compromise. Once an agency has detected the compromise, it must take actions to attempt to collect any improper payments.

Even if the compromise is detected in a timely manner, the impacts can be catastrophic to an agency's operations regardless of whether a loss of funds occurs from the compromise. [PKI-039]

As we have noted, systems must be set up to positively identify internal and external users, issue them digital certificates, and manage the exchange and verification of certificates. Should the certification authority be compromised, the agency would have to go through the time consuming and costly process of reissuing digital certificates in accordance with the agency's policies and procedures.

Certificates used for critical financial management applications should be issued based on split knowledge and dual control concepts and the individual's identity should be validated by personally appearing before the registration authority. **For some agencies a compromise could mean reissuing tens of thousands certificates. If an agency has integrated its PKI into its systems, a significant disruption can result if the agency has to shut down associated systems because of a compromised PKI.** For example, users may not be able to use those systems until they have received new certificates. In a non-PKI context, when one agency decided to shut down its financial management operations so that it could convert to a new system, we understand that the agency incurred over \$1 million in late payment penalties as a result of the financial management system not being available. When the system has PKI, even if the agency bypasses the existing control process, the agency exposes itself to other attacks since the system is no longer using one of its critical control techniques to ensure data integrity—the PKI. Regardless of the decision, the agency is exposing itself to increased risks by (1) not processing transactions or (2) processing transactions without an adequate level of data integrity. ...

In cases where a certification authority is compromised, the agency should have recovery plans in place to mitigate the damage. As a part of each agency’s information security program which OMB

⁷¹ Rhodes, K. A. *Public Key Infrastructure: Examples of Risks and Internal Control Objectives Associated with Certification Authorities*. Tech. Rep. GAO-04-1023R, United States Government Accountability Office, Washington, DC 20548, August 2004. Available at <http://www.gao.gov/new.items/d041023r.pdf>

must approve, agencies are required to have plans and procedures to ensure continuity of operations for information systems that support agency operations and assets, regardless of whether those operations and assets are managed by another agency, contractor, or other source.

Though necessary to ensure continuity of operations, the implementation of a plan to address the compromise and recover the necessary PKI functionality may likely cause an agency to incur significant costs.

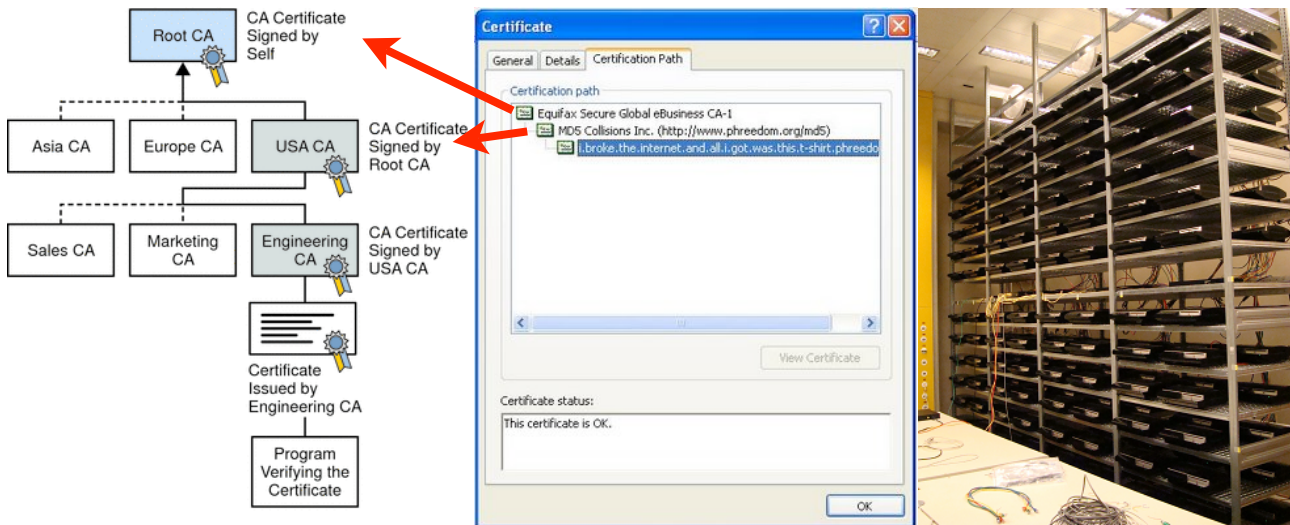
We observe that in the case of civilian PKI systems: “Any Certificate authority can usurp a certificate issued by any other CA. The overall security is that of the least trustworthy CA”⁷². [PKI-021] More on this below.

6.3.3 Has the exploitation of a single-point of trust failure in PKI Based ID systems been demonstrated in the real world?

YES.

Many commercial Certificate authorities, each with “GLOBAL” name-space authority, emerged. Instead of having a single point of trust failure in Kerberos like SKD systems, we now have well over 20 root certificate authorities, and if any of those 20+ authorities goes rogue it can undermine and attack any website, in any nation, in any domain name space (.eu, .ru, .cn, .mil, ...). The global civilian community can be held to ransom if one authority is for whatever reason caused to go ‘rogue’ and through one authority one party can wage cyber war against the majority. [PKI-021] [PKI-024]

This vulnerability in the current public key infrastructure was clearly demonstrated with the well published MD5 rogue certificate authority attack.



The middle panel above shows a forged Certificate, which is accepted by the Windows Operating System which states: “This certificate is OK.” See MD5 Collisions Inc. (<http://www.phreedom.org/md5>) The right panel shows the cluster of Sony Playstation 3’ devices that were used to find the MD5 collision which led to the rogue Certificate Authority, which in turn could generate fake certificates for any website on the Internet.

The lack of end-to-end redundancy in modern PKI has led to systems that place the global civilian community at risk of abrupt and potentially catastrophic security failures/attacks at the hands of a few.

This fuels the risk of cyber crime and potentially cyber war.

⁷² Gutmann, P. *Everything you never wanted to know about PKI but were forced to find out*. Available at <http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf>, page 21.

There is an obvious need for end-to-end redundancy and this should not just provide multiple independent international service providers for freedom of choice, it should also provide multiple independent national service providers to remove single points of potential catastrophic failure for national and international secure traffic. [SPOTF-003] Currently any business could be a victim of a cyber attack from any other nation which has this unrestricted power to act unilaterally.

We argue that at least in the case of international transactions (and preferably in all transactions), a citizen's or a company's privacy and security should not be subject to any single organisations/nations authority. [SPOTF-001] [SPOTF-002] [SPOTF-004] We argue for a new model that distributes trust with end-to-end redundancy for Identity Management and Cryptographic Key Management, so that an attack against an individual should require international collaboration. This type of technology can also prevent the rise of authoritarian states.

6.3.4 Can we defend against single points of potential trust failure?

*“Research on new approaches to achieving security **and resiliency** in information and communications infrastructures is insufficient. The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs **and national security requirements**.”*

– US 60-day Cyberspace Policy Review

YES. Today, modern security research agendas in the EU and US are calling for resiliency. Systems with system-wide single point of trust failures (or systems with localised single-point of trust failures that influence hundreds of thousands of users) are not resilient. Unfortunately, as illustrated above today's public key infrastructure falls into this category, including the OpenID and the U.S. Federal PKI bridge initiatives.

An effective way to achieve resiliency is to consider applying “separation of powers” and distributing trust across those powers by using end-to-end redundancy. This singular design factor radically influences the architecture of information processing systems including ID management, Cryptographic Key Management and all systems that must manage trust.

Recurring theme:

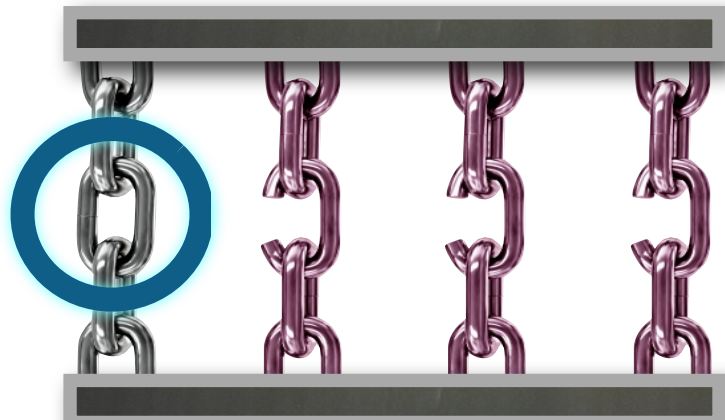
Single point of (potentially system wide) trust failures

Problem:



System fails catastrophically when one component fails...

Solution:



Use End-to-End redundancy with independent chains of trust...

“In my opinion, using redundant means to produce security is an idea that warrants more attention than it receives -- provided, of course, that the cost is reasonable.”

– Prof. Martin Hellman, co-inventor of Public Key encryption, personal correspondence, 2010

Image of chains © iStockPhoto. Used with permission.

6.3.5 What does an end-to-end secure cryptosystem look like?

Traditionally it is said that the strength of a security system is as strong as its weakest link. Cryptographic systems typically rely on one algorithm (to perform a given function) and for example practically the entire global community gambles the continuity of the Internal/Global Market on public key cryptography. The absence of redundancy means that if that algorithm breaks then the entire global system catastrophically collapses. Furthermore, the current practice that centralises trust (for millions of users or even the entire system) into a single authority or bridging authority limits international collaboration and provides yet another single point of potential catastrophic failure. Previously such systems were preferred to optimise performance but advances in computing efficiency and reducing costs make redundancy far more cost effective today.

Former US NSA Senior Technical Director Brian Snow is on the record as stating that *“today’s software security industry can be likened to a car in the 1930’s. It looks good, it goes fast, but in an accident you die.”* We all employ redundancy with data backups but we have no redundancy in the cryptography or protocols in our global security systems.

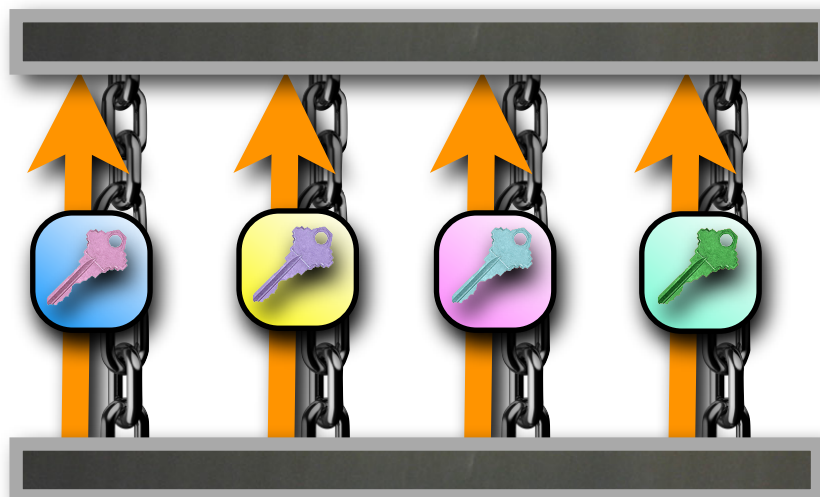
Now of course publications from various US cyber initiatives (such as NIST CKM Workshop) have identified that our ‘fast’ PKI based key exchange systems have actually resulted in a transfer of various difficult responsibilities such as key management to the end user and the complexities involved are a hindrance to the ubiquitous take up of encryption! [PKI-040]

Reaching agreement between competing nation states and corporations about whose/which cryptographic algorithms to use creates major obstacles to international collaboration, particularly at the Government level ⁷³. [PKI-041] A multiply redundant international protocol could shift trust from one central point of control and single algorithm that both represent single points of potential catastrophic failure.

Existing international systems such as PKI based certificate authorities are exposed to catastrophic failure because every authority in any country has the ability to falsify any domain name or website across the globe. One nation or service provider should not have the capability to hold the international community to ransom. [PKI-025]

So how might we begin to address these above problems?

In 1976, the three cryptographers Whitfield Diffie, Martin Hellman and Leslie Lamport wrote a paper called "Multiuser cryptographic techniques" ⁷⁴, which describes a **free-to-use** ($m-1$) computationally secure symmetric key distribution (SKD) scheme that uses m key distribution centres. This new idea distributed trust across m different servers. As partially illustrated below, the scheme enabled two users to securely distribute m different portions of a key across m different paths, and reconstruct it (using a cryptographic hash to secure mix together the concatenated value of the m keys) so that only the sender and receiver knew the final value, in this case $m=4$.



⁷³ Ballard, M. *EU crypto project SUPHICE mired in red tape*. SearchSecurity UK (Jan 2008). Available at http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1289573,00.html

⁷⁴ Diffie, W., and Hellman, M. E. Multiuser cryptographic techniques. In AFIPS '76: Proceedings of the June 7-10, 1976, national computer conference and exposition (New York, NY, USA, June 1976), ACM, pp. 109–112. Available at <http://doi.acm.org/10.1145/1499799.1499815>

As illustrated in the solution on the previous page, this scheme is secure while ever 1 of the m servers refuses to collude with the other $(m-1)$ servers. This process can be implemented such that each of the servers is owned, run and maintain by a different Nation State. For example, in a hypothetical international scheme the $m=6$ servers could be run by the competitive states Israel, Palestine, France, Germany, Russia, China. Users of the system may have a reasonably high level of confidence that illegal collusion between the six states is unlikely to occur.

The concept of $(m-1)$ redundancy was known at the time and could have been applied to public key infrastructures when they were introduced. Unfortunately first generation solutions were either commercially motivated with a view to dominate the market (Verisign was founded by one of the makers of RSA and not Diffie, Hellman, Merkle or Lamport), or based in a Government model of single point of top-down command and control mentality. Computer performance and cost was also issues at the time but these barriers to redundant systems can be shown to be no longer an issue. The benefits of redundancy far outweigh and minor performance reduction.

Today the retroactive application of $(m-1)$ redundancy in public key infrastructures has limited short-term value because of the known quantum computing threats to all standards based public key cryptography which would put a limited life time on this corrective action. The effort to fix single-point-of-trust problem in an infrastructure that has known catastrophic future risks **is not cost effective**. The known mid-to-long term threats are the reason given by the NIST CKM Project Leader Elaine Barker for her call at the NIST CKM Workshop for the study of symmetric solutions that do not rely on PKI. [PKI-042]

[Intentionally left blank]

6.3.6 Are there examples of trust models that permit a relatively weak individual to trust a powerful organisation?

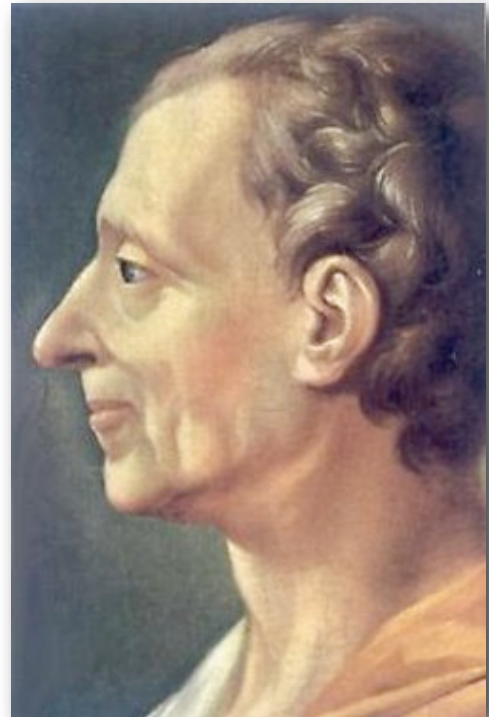
YES.

We observe that this type of ($m-1$) secure cryptosystem can be seen to be an expression of “separation of powers” and a system of “checks and balances” as articulated in the book “The Spirit of Laws”⁷⁵.

The Spirit of Laws (French: L'esprit des lois) is a [treatise on political theory first published anonymously](#) by [Charles de Secondat, Baron de Montesquieu](#) (public domain image illustrated to the right) in 1748.

Montesquieu spent nearly twenty years researching and writing L'esprit des lois (The Spirit of the Laws), covering a wide range of topics in politics, the law, sociology, and anthropology. In this political treatise Montesquieu advocates constitutionalism and the separation of powers, the abolition of slavery, the preservation of civil liberties and the rule of law, and the idea that political and legal institutions ought to reflect the social and geographical character of each particular community. All these fundamental principles remain as valid today as they did in 1748.

It is these principles that has led to the design of Governments that permit individual citizens of limited means to have some level of trust in the integrity of their Governing system. It is arguable that these same principles can be applied to next generation security systems to provide trustworthy systems to protect the diversified interests within and across the global community.



In Book III, Part 1, “*Difference between the Nature and Principle of Government*” in comparing the various political models of Democracy, Aristocracy, Monarchism and Despotism, Charles observes:

“The nobles form a body, who by their prerogative, and for their own particular interest, restrain the people; it is sufficient that there are laws in being to see them executed. But easy as it may be for the body of nobles to restrain the people, it is difficult to restrain themselves. Such is the nature of this constitution, that it seems to subject the very same persons to the power of the laws, and at the same time exempt them.”

“For it is clear that in a monarchy, where he who commands the execution of laws generally thinks himself above them, there is less need of virtue than in a popular government, where the person entrusted with the execution of the laws is sensible of his being subject to their direction”.

We observe that the design of security systems by financial institutions, very large commercial organisations, national institutions or military institutions may be likened to the systems governed by Aristocracies. These systems tend to shift liability and provide advantage and reduced accountability to the most powerful actor⁷⁶. [SPOTF-006]

In contrast, and in away more akin to that of popular democracy, we assert that to achieve a *virtuous* identity management/cryptographic key management/security system, the policies and procedures codified in their architecture must be designed in a balanced way to take into account the legitimate interests of all stake-holders, to ensure accountability for all stake-holders, and prevent liability shifting or the granting of advantage for commercial or national interests. [PKI-007]

⁷⁵ de Secondat, Charles, B. d. M. The Spirit of the Laws (Originally published anonymously in 1748). Crowder, Wark, and Payne, 1777. Available at <http://socserv.mcmaster.ca/econ/ugcm/3ll3/montesquieu/spiritoflaws.pdf> and <http://www.constitution.org/cm/sol.htm>.

⁷⁶ Anderson, R. J. Liability and computer security: Nine principles. In ESORICS '94, Springer-Verlag, pp. 231–245. Available at <http://www.cl.cam.ac.uk/~rja14/Papers/liability.pdf>.

6.3.7 What is the code-breaking quantum computing threat?

6.3.7.1 A Preliminary word on the code-breaking quantum computer threat

Many small quantum computers exist today in laboratories around the world. Private investors, Governments and National Security Agencies are funding further research into finding code-breaking quantum computing. [PKI-036]

Code breaking quantum computers are « **understood to be an issue that is already visible as a possible future risk to network and information security** » and that this threat presents a « **significant risk of undermining the smooth functioning of the Internal Market** » as it anticipated to undermine the security mechanisms of almost all security systems in the market.

There are NO KNOWN Public Key Distribution schemes currently considered suitable by the international community for use after the arrival of code-breaking quantum computers. **This is an OPEN PROBLEM.** [PKE-007]

We advise that addressing the quantum computing threat DOES NOT require quantum key distribution.

The Quantum computing threat is a long-range event (9+ years) [PKE-003] that could have devastating impact on data generated 5 years from now. Large organisations and government bodies require a >5 year duration of data security and may take more than a decade (such as EMVco) to upgrade to a protect against quantum computing threats.

The code-breaking quantum computing threat is an **INDEPENDENT** threat that exists **OVER-AND-BEYOND** the existing Single Point of Trust Failures in public key cryptosystems.

When the two different threats against public key technologies are considered together, there is doubt whether this technology is capable of ensuring the ongoing smooth functioning of the Internal Market in the mid to long-range future.

The risk of code-breaking quantum computers is particularly relevant to long-range EU funded projects such as SESARJU and national security systems.

6.3.7.2 What is the future threat posed by code-breaking quantum computers?

Brian SNOW

Peter SHOR

"The [ed. quantum] threat to cryptography is well understood due to work by (Peter) Shor and others

A **symmetric algorithm** like AES or other standard crypto processes is **cut key-size in half**, which is a **dramatic reduction**..."

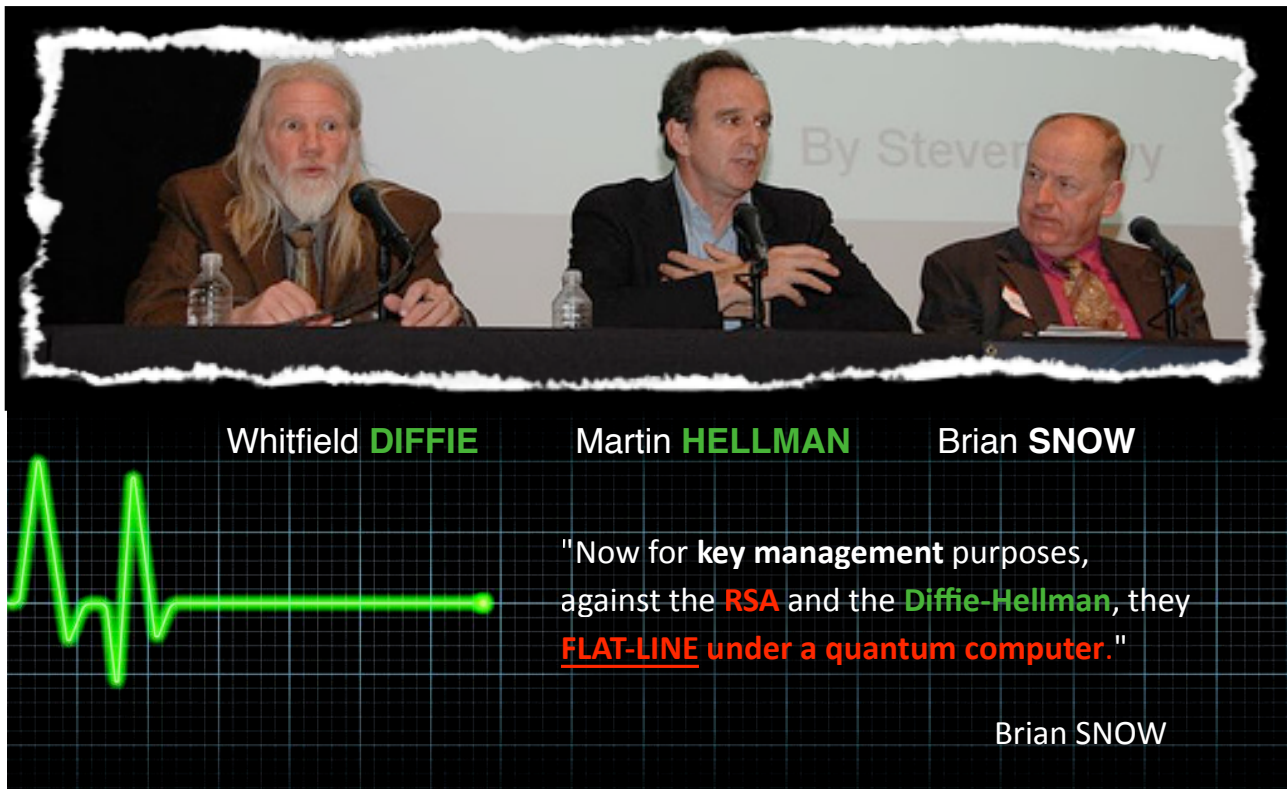
Brian SNOW
Former Technical Director of the Information Assurance Directorate, US NSA

Code breaking quantum computers damage all symmetric key algorithms, but this can be compensated for in practice. In *practice* quantum computers are *just another attack* that has to be taken into account when deploying symmetric ciphers like 3DES and AES-256.

(Image of Brian Snow: <http://flickr.com/photos/farber/280651148/>, <http://www.flickr.com/photos/farber/>, <http://creativecommons.org/licenses/by-nc/2.0/>) (Image of Peter Shor from: <http://www-math.mit.edu/~shor/>)

This means that addressing the code-breaking quantum computing threat DOES NOT REQUIRE quantum key distribution because we can use NIST ciphers like the Advanced Encryption Standard with a 256-bit key.

But for Government approved public key cryptography:



Whitfield **DIFFIE** Martin **HELLMAN** Brian **SNOW**

"Now for key management purposes, against the **RSA** and the **Diffie-Hellman**, they **FLAT-LINE** under a quantum computer."

Brian SNOW

(Image: <http://www.flickr.com/photos/63251347@N00/280651254/>, <http://www.flickr.com/photos/farber/>, <http://creativecommons.org/licenses/by-nc/2.0/>)



Code breaking quantum computers are a “**nightmare**” for IT Security. All mainstream public key algorithms are dead. [PKE-001]

Professor Johannes Buchmann:
Technische Universität Darmstadt
World leading post quantum security expert
(Image: TUD)



Standards based public key crypto CANNOT be upgraded today:

“**an open problem**
... an aching problem” [PKE-007]

Brian Snow (2006)
Former Technical director of the Information Assurance Directorate of the NSA.
(Image: ZDNet.com.au)

Does the EU have a risk management strategy in place to manage the situation when all certification authorities are compromised due to quantum computer so the community can mitigate the damage?

6.3.8 Long range significance of code-breaking quantum computers on National Security Systems

The robust and continued operation of National Security Systems and Critical Infrastructures are necessary to support the European Community. Disruption of these systems could lead to disturbances in global stability. In some cases, such as with nuclear power stations and military Physical Access Control Systems, many lives can be put at risk if the confidentiality, integrity or availability of these systems is compromised.

It is known that the ICAO MTRD (e-passport) program (used by the EU) relies on public key cryptography. The EU STORK⁷⁷ program has surveyed the national ID schemes used by member states. Many ID schemes have been identified by STORK to rely on public key cryptography. It is known that the US Personal Identity Verification card (FIPS 201) relies on public key cryptography. It is known that biometrics are protected using at risk public key cryptography. Also according to Kathleen KRANINGER, Director of Office of Screening Coordination at the Department of Homeland Security in the United States at a presentation at CARTES 2008, access to Nuclear Facilities are secured using public key technologies.

In all these cases, the public key cryptography used is known to be at risk from Shor's quantum algorithm.

The EU, US and China Governments are actively funding the research and development of code-breaking quantum computers. [PKI-036] Yet the EU, US and China continue to deploy security systems that rely on the public key cryptography that the Government funded quantum computing research initiatives are specifically trying to break. [PKI-003]

National intelligence organisations such as the US NSA support quantum research:

“And what they do is remarkable. Since one qubit can simultaneously represent two different values, two qubits can simultaneously represent four (00, 01, 10, and 11, in binary notation); four qubits can represent 16 values; eight qubits 256 values; and so on. Even a relatively small quantum computer, one that had a few tens of thousands of qubits, could consider so many different values at once that it would be able to break all known [ed: RSA, D&H, ECC, AES-128] codes commonly used for secure Internet communication. Quantum computers might also be used for faster database searches, or to tackle hard problems that classical computers couldn't solve with all the time in the universe. My colleagues at MIT and I have been building simple quantum computers and executing quantum algorithms since 1996, as have other scientists around the world. Quantum computers work as promised. If they can be scaled up, to thousands or tens of thousands of qubits from their current size of a dozen or so, watch out!”

“Given their power to intercept and disrupt secret communications, it is not surprising that quantum computers have the attention of various U.S. government agencies. The National Security Agency, which supports research in quantum computing, candidly declares that given its interest in keeping U.S. government communications secure, it is loath to see quantum computers built. On the other hand, if they can be built, then it wants to have the first one.”

– Professor Seth Lloyd of MIT 2008⁷⁸

If just one (open or closed) code-breaking quantum computing research project is successful, that group can provide code-breaking and forgery services to Governments, national intelligence organisations, military organisations, or terrorists anywhere in the world. [PKI-043]

At that time, it will be as though there are no confidentiality or integrity mechanisms implemented in national security and critical infrastructure systems. It will be as though no authentication of identities has been performed.

The security of the e-Passports reverts back to the security of un-chipped passports. The security of biometric e-Passports reduces to less than un-chipped passports as fake biometrics can allow users to pass through automated electronic access gates. Remote monitoring and management systems of critical infrastructure will be compromised, exposing the system to the will and caprice of malice agents. These systems may be forced to disable safety mechanisms and fail in physical ways that could harm the lives of those living near these systems.

As President Obama said at the Nobel Peace Prize Ceremony, Oslo, 10 December 2009; *“modern technology allows a few small men with outsized rage to murder innocents on a horrific scale.”*

⁷⁷ <https://www.eid-stork.eu/>

⁷⁸ <http://www.signallake.com/innovation/RidingD-Wave042408.pdf>

6.4 Background information on current and emerging US and EU research and development agendas

6.4.1 RISEPTIS call for a common European ID Framework

6.4.1.1 About RISEPTIS

Think-Trust (T-T) (www.think-trust.eu/) is an F5 Coordination Action under Framework Program 7 (FP7) Challenge 1, Objective ICT-2007.1.4 – Secure, Dependable and Trusted Infrastructures. T-T has been allocated the task of helping to coordinate the response to the needs of a trustworthy ICT future in Europe, through working groups, surveys and consultations resulting in Reports with recommendations and priorities about what needs to be done. Its target audience is the European Commission and policy-makers responsible for future direction, strategies, and priorities for European ICT. T-T deliverables complement the RISEPTIS (Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society) work by providing feedback on priorities based upon input from their various activities, and input from the perspective of participants in the European ICT Framework Programme.

The T-T project includes the support of an Advisory Board, "Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society" - RISEPTIS (<http://www.think-trust.eu/riseptis.html>). RISEPTIS is a high-level advisory body in ICT research on security and trust aiming at providing visionary guidance on policy and research challenges in the field of security and trust in the Information Society. It will do so by formulating recommendations on:

- Policy environment – The development of coherent legal and administrative frameworks, operational environments, and human behaviour relating to security, privacy and confidence, in view of the technological changes leading to and arising from the future Information Society,
- Research Agenda – Future European research and development that can facilitate the creation of an Information Society that will be secure, whilst respecting freedom and privacy of its citizens, with due attention given to the ICT infrastructures, networks, services and applications.

6.4.1.2 Recommendations made by RISEPTIS

According to the October 2009 RISEPTIS Report⁷⁹ entitled “*Trust in the information society*”: “*The trustworthiness of our increasingly digitised world is at stake.*” Furthermore: “*if citizens feel threatened, mistrustful and increasingly hesitant towards innovative applications and services, our whole society may end up being the loser.*”

The Report makes 6 recommendations, and we highlight 2 of those 6 that relate to identity management.

Recommendation 1:

The EC should stimulate interdisciplinary research, technology development and deployment that addresses the trust and security needs in the Information Society. The priority areas are:

- Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet
- Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability
- Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography)
- Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management

Recommendation 3:

The EC, together with the Member States and industrial stakeholders, must give high priority to the development of a common EU framework for identity and authentication management that ensures compliance with the legal framework on personal data protection and privacy and allows for the full spectrum of activities from public administration or banking with strong authentication when required, through to simple web activities carried out in anonymity.

⁷⁹ <http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html>

6.4.1.2 Benefits of a Unified ID framework proposed by RISEPTIS

According to RISEPTIS:

“Trust is at the core of social order and economic prosperity. It is the basis for economic transactions and inter-human communication. The Internet and the World Wide Web are transforming society in a fundamental way. Understanding how the mechanisms of trust can be maintained through this transformation, is of crucial importance.”

“We see trust as a three-part relation (A trusts B to do X). Parties A and B can, in this respect, be humans, organisations, machines, systems, services or virtual entities. Trustworthiness relates to the level of trust that can be assigned to one party (B) by another party (A) to do something (X) in a given relational context.”

“The first steps towards cooperation have already been launched by the Commission to ensure an interoperable and trustworthy ID management platform in Europe⁸⁰, following joint efforts of Member States in the project STORK⁸¹.”

RISEPTIS also quotes “The laws of identity”:⁸²

*“1. **User Control and Consent:** Technical identity systems must only reveal information identifying a user with the user’s consent.*

*2. **Minimal Disclosure for a Constrained Use:** The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.*

*3. **Justifiable Parties:** Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.*

*4. **Directed Identity:** A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.*

*5. **Pluralism of Operators and Technologies:** A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.*

*6. **Human Integration:** The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.*

*7. **Consistent Experience Across Contexts:** The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.”*

A unified ID framework is required to ensure a consistent experience across contexts.

A unified ID framework is required so that parties can accurately identify each other when required.

A unified ID framework is required to manage the control of personal data through its entire life cycle.

A unified ID framework is required to manage accountability of the actions of humans and devices.

As illustrated in Section 6.3, an evolutionary approach to identity management using existing standards based security systems as a platform will result in deployment of identity systems that are known to be risk of single points of potential trust failure that could affect the integrity of the global system, and could entirely collapse with the advent of code breaking quantum computers. [PKI-043]

⁸⁰ COM (2009)116: A Strategy for ICT R&D and Innovation in Europe: Raising the Game

⁸¹ <http://www.eid-stork.eu/>

⁸² See: <http://www.identityblog.com>

6.4.2 US 60-day Cyberspace Policy Review

One of U.S. President Obama's first acts was to order a 60 Day Cross Government 'clean slate' Cybersecurity Review. On the 29th of May 2009, President Obama presented the US Federal Cyberspace Policy Review Report.

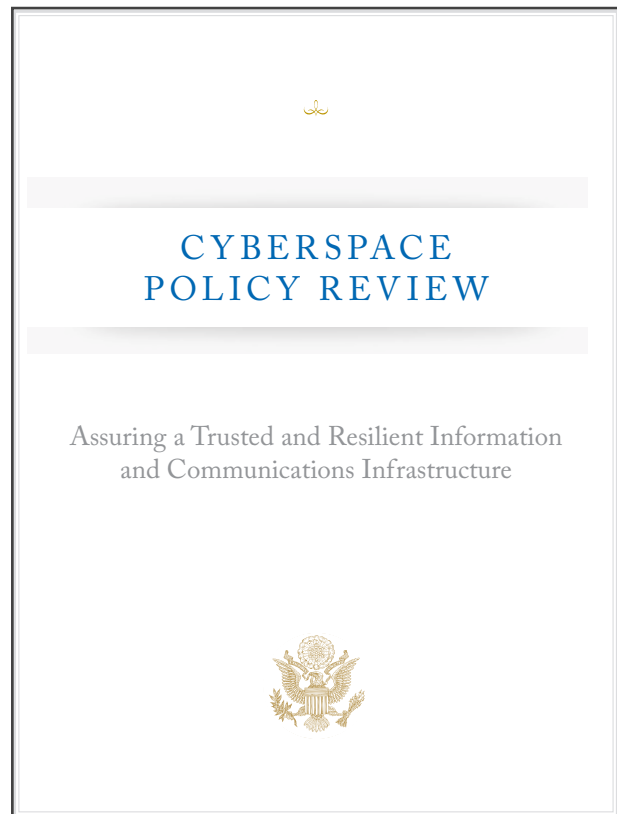
The Report concluded:-

“Cyberspace touches practically everything and everyone. It provides a platform for innovation and prosperity and the means to improve general welfare around the globe. But ... great risks threaten nations, private enterprises, and individual rights ... The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient.”

The report included a 10 point near term action plan.

Point 9: *“In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.”*

Point 10: *“Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.”*



Impact of the Cyberspace Policy Review

Two important cybersecurity activities in the United States have followed rapidly on the publication of the Cyberspace Policy Review Report.

Acting on above mentioned points 9 and 10:

- The U.S. Government's National Institute of Standards and Technology (NIST) held an official Cryptographic Key Management (CKM) workshop⁸³ to: [PKI-005]

“improve the overall key management strategies used by the public and private sectors in order to enhance the usability of cryptographic technology, provide scalability across cryptographic technologies, and support a global cryptographic key management infrastructure”.

“There is a major need to support key management as part of the national cyber security initiative”. (June 2009)

- The U.S. Government's Networking and Information Technology Research and Development Program (NITRD) held the National Cyber Leap Year (NCLY) Summit on 17 to 19 August 2009 in Arlington, Virginia to find game changing ideas.

⇒ **Key management intrinsically relies on Identity management.**

⁸³ http://csrc.nist.gov/groups/ST/key_mgmt/

6.4.3 United States Cryptographic Key Management (CKM) project [PKI-005]

6.4.3.1 About the National Institute of Standards and technology (NIST) CKM

Quotes from http://csrc.nist.gov/groups/ST/key_mgmt/:

“There is a major need to support key management as part of the national cyber security initiative”. (June, 2009)

“Cryptographic Key Management (CKM) is a fundamental part of cryptographic technology and is considered one of the most difficult aspects associated with its use. Of particular concern are the scalability of the methods used to distribute keys and the usability of these methods. [PKI-030]

NIST has undertaken an effort to improve the overall key management strategies used by the public and private sectors in order to enhance the usability of cryptographic technology, provide scalability across cryptographic technologies, and support a global cryptographic key management infrastructure.”

“A CKM Workshop was held at NIST on June 8-9, 2009. Approximately 100 people participated in the Workshop at NIST on-site and approximately 90 people participated via a Webcast service. The program consisted of five keynote speakers addressing various aspects of future electronic communications, computing, and cryptography. Another twenty-five speakers addressed various technical aspects of current and future key management systems including key management policies, algorithms, distribution methods, and user control software interfaces.”

“The CKM workshop was initiated by the NIST Information Technology Laboratory’s Computer Security Division to identify technologies that need to be developed that would allow organizations to ‘leap ahead’ of normal development lifecycles to vastly improve the security of future sensitive and valuable computer applications.”

6.4.3.2 Requirements and Anticipated Benefits of the NIST CKM initiative

We have identified the following 5 core points articulated by senior NIST representatives at the Workshop as the reason for the CKM Project. Many of these core points are also expressed by industry at the NIST CKM Workshop.

1. **New and improved solutions that are focused on the user**

NIST Quotes: *“user friendly”, “easy to use”, “plug and play”, “user driven”*

NIST Quote: *“It is not acceptable to only have a choice between usability with little security and security with little usability. A CKM system designer has to know the prospective user and to understand that security is not the primary task of the user. A system must be efficient, effective and understandable. There is no complex system that is secure.”*

2. **Scalable solutions**

NIST Quote: *“We know how to handle key management reasonably effectively for up to a million people, we need to go a couple of orders of magnitude beyond that in the relatively near future”*

NIST Quote: *“Identity based symmetric keys may reduce the scale of symmetric key distribution problem”*

3. **Vastly improved security**

NIST Quote: *“We’re not going to accept high risks in the future Internet, because we don’t want the adversaries to have high payoffs.” [PKI-030]*

NIST Quote: *“We need resilience against quantum computing attacks” [PKE-002]*

NIST Quote: *“... to identify technologies that need to be developed that would allow organizations to ‘leap ahead’ of normal development lifecycles to vastly improve the security of future sensitive and valuable computer applications.”*

NIST Quote: *“We also need key inventory control, accountability/auditing of the keys, policies for managing the keys and metadata, and safety requirements for certain applications”*

NIST Quote: *“... must be secure, cost-effective, fault-tolerant, and highly available”*

NIST Quote: *“... must look at means other than using public key-based key management systems”*

4. **Fault-tolerant, highly available**

NIST Quote: *“Survivable key management systems” [SPOTF-003] [SPOTF-004] [SPOTF-006]*

5. **Cost-effective**

NIST Quote: *“Executive and legislative oversight and resource allocation must be in the proper context. Expectations must be consistent with technical reality. We must work with industry, not just from the standpoint of innovation and technical expertise, but making sure the standards that result will be implemented, not just can be implemented.”*

6.4.4 SESARJU and NextGen

6.4.4.1 About SESARJU and NextGen

SESAR (Single European Sky ATM Research) http://www.eurocontrol.int/sesar/public/subsite_homepage/homepage.html marks the planned shift from radar to global positioning air traffic control amongst many other technological advances. The equivalent U.S. Next Generation Air Transportation System (NextGen), like SESAR, is a transformation of national airspace systems, including the system of airports, using 21st century technologies to ensure future safety, capacity and environmental needs are met. SESARJU and NextGen are future technologies under development today.

« SESAR is one of the most important research and development projects ever launched by the European Union - While the Single European Sky's regulations will provide a revised legal framework for a more efficient, performance driven, safer and greener procedures for the air traffic management, the SESAR programme will deliver technological solutions, functionalities, systems and standards which will be deployed in Europe. »

– Daniel Calleja – Director Air Transport Directorate – European Commission

Cyberspace security will be even more critical than ever before in future air traffic control. As a very expensive long term critical infrastructure project it is essential that equally long term high assurance cybersecurity is deployed to protect the massive investments required and all air travel consumers. Cybersecurity initiatives in the US are already identifying risks and future needs that must be recognised and accommodated in this project to ensure international co-operation and acceptance and to ensure that the project remains secure during its projected 30+ year serviceable life.

| Single European Sky ATM Research – Joint Undertaking | | |
|--|--------------------------|----------------------|
| Started | 2004 | |
| Definition Phase | 2006 → 2008 | |
| Development Phase : TODAY | 2008 → 2016 | € 2.1 billion |
| Deployment Phase | 2013 → 2025 | |
| Operational Life | AT LEAST 30 YEARS | |

This is not the “full” cost to the global community. According to Luc Lallouette, SESAR Programme Director for the R&D phase at Thales, the SESAR project must be applicable globally. This includes the requirement that SESAR and US NextGen initiatives must be interoperable with each other.

The US Federal Aviation Authority (FAA) is soliciting bids from companies interested in competing for NextGen support contracts with an approximate combined value of **\$7 billion**, the largest award in the agency’s history. Under the umbrella awards, called System Engineering 2020 (SE2020), the FAA will award as many as five separate contracts for **research and development** and **systems engineering** work that will help the agency deliver NextGen.

6.4.4.2 Benefits of SESARJU and NextGen

The high level goals of these two project are to:

- Increase capacity and reliability
- Improve safety and security
- Minimise the environmental impact of aviation

These are quantified as:

- An improvement in safety by a factor of 10
- Support 3 times more traffic
- Cut ATM costs by 50%
- Reduce environmental impact 10% per flight
- A 8 to 14 minutes reduction in flight time on average
- Cut air traffic management costs by 50%

These improvements to the air transportation system will be achieved by applying:

- Space-based navigation and integrated surveillance

- Digital communications
- Layered adaptive security
- Weather integrated into decision-making
- Advanced automation of Air Traffic Management
- Net-centric information access for operations

These projects are seeking to reduce the amount of manual labour required to manage air traffic. Features of the new **electronic** systems include new Trajectory Management functions, Separation Modes, Controller Tools and Safety Nets, Airspace Management supporting functions, Management Complexity tools, Queue Management and Route optimisation features. This also includes functions such as Optimized Profile Descent for aircraft seeking to land, which also requires synchronisation movement of flight in air and on ground.

The number of flights is rising rapidly and the European future economy is based heavily on tourism which relies on flights.

The integrity and availability of flight control systems is critical to ensuring the increased capacity can be managed safely.

These flights must be safe, otherwise the stability of the Internal Market may be damaged.

6.4.4.3 Known Security Risks in existing Aviation systems

TODAY: Under the auspices of the Air Transport Association (ATA), the aviation industry has standardised security credentials for authentication, digital signatures, and encryption. The ATA's Digital Signature Working Group (DSWG) has created an aviation industry wide public key infrastructure (PKI) standard, ATA Specification 42. Specification 42 defines a PKI certificate standard for the aviation industry, using a type of public key encryption called Elliptic Curve Cryptography. This is part of the US NSA Suite B⁸⁴ set of international security standards promoted by the America for securing up to CLASSIFIED information. ECC is known to be at risk from code-breaking quantum computers. [PKE-010]

The ATA DSWG has also established a PKI bridge under CertiPath to allow any two members of the aviation industry to exchange security credentials. The group has done extensive work on defining the exact format of the digital certificates that are used by the Certificate Authority in order to maximise interoperability and aviation functionality.

All air and ground technologies using PKI is known to be at risk. The PKI bridge is known to be at risk from single points of potential trust failure. Furthermore, the PKI technologies uses are at risk from code-breaking quantum computer attacks that experts such as Prof. Seth Lloyd (who led the team to build the first quantum computer) may arrive in approximately 9 years.

TODAY: System-Wide Information Management (SWIM) is an information technology program that identifies industry standards and commercially available products to ensure interoperability between National Airspace System systems. This will improve operational decision making because it will be easier to share data between systems. SESAR-WP8 is responsible for Information Management Work Package and concerns the "Intranet for ATM". SESAR-WP14 is responsible for defining the SWIM technical architecture. WP14 is required to support WP8. P14.2.2 will have to face the challenge of making the SWIM network safe and secure.

One of the known SWIM Challenges⁸⁵ is that selected military ground systems lack the required level of interoperability to provide connectivity and exchange services with the IP-based ground communications Pan-European Network Services (PENS). This type of interoperability problem between new and legacy systems will increase with the mandatory upgrade of security protocols in response to known quantum computing threats.

If the SWIM security model takes an evolutionary approach using existing aerospace security standards based on Public Key Cryptography and Public Key Infrastructures, then the SESARJU and NextGen cryptographic security components will known to be at risk before they were developed. [PKI-003]

⁸⁴ http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

⁸⁵ Altran Group. *Feasibility studies on the integration of military ground and aircraft systems in the SESAR concept and architecture*, "Capability gaps between military systems and SESAR". Executive summary, Eurocontrol, October 2008. Available at http://www.eurocontrol.int/mil/gallery/content/public/milgallery/documents/ALTRAN%20brochure%20Final_OCT08.pdf

7. Benefits

Brief description of the benefits likely to emerge from this assessment report.

7.1 The empowering benefits to the EU community of a comprehensive risk management report on PKI

THE EU COMMUNITY IS MARGINALLY SECURE TODAY

THE EU COMMUNITY IS TOTALLY UNPREPARED FOR THE FUTURE COMPUTING TECHNOLOGIES THE EU COMMUNITY IS FUNDING AND DEVELOPING

To the best of our knowledge, a comprehensive study of the RAMIFICATIONS of the current deployment and continued deployment of PKI systems to the stake holders in the EU community has not been performed.

Current and immediate future (Public Key Infrastructure + Single point of trust failure)

1. It would provide an **authoritative, independent establishment and confirmation of the known weaknesses of PKI**. It would **highlight the unacceptable risks and ramifications of relying on security systems with system wide single-point-of-trust failures** that can effect the entire EU community.
2. The report would **mitigate continued non-action by calculating and articulating the risks and potential negative impacts** from the loss of security and privacy, and the roll-on negative economic impact to EU Nations and stakeholders as a result of not immediately addressing the known weaknesses posed by PKI.

There are no known approximations of how much each stakeholder stands to lose due to a requirement or component of the system failing on account of the various known risks to PKI. [PKI-044]

The value of a risk management report of this nature is that it can identify vulnerabilities and provide options to mitigate these vulnerabilities at their earliest stages before they become more pernicious. In addition such a study could provide a quantitative indication of reliability, performance, and/or safety of a system accounting for the criticality of each requirement as a function of one or more stakeholders' interests in that requirement^{86, 87}.

3. Once we are able to consider **the mean failure cost for each stakeholder** (which is the cost we expect to incur as a result of the lack of security), this loss **can be balanced against the cost of improving system security**. In this way a well-formed risk assessment report can provide an estimate of an appropriate amount to spend to address the known threats.

The report should enable a clear return on investment for the different proposals to be calculated.

4. A risk management study **would support the existing EU calls (SecureIST) for the development of a universally acceptable hardened information technology infrastructure** that can provide MEDIUM to LONG-TERM assurances (50-to-100 years).
5. The outcome of such a study by ENISA on PKI **would feed into the Unified Identity Framework proposed by the RISEPTIS, and influence the design of security mechanisms in SESARJU development efforts** and could potentially influence every segment of the European and the electronically connected Global community.
6. The ensuing benefits from a report that **instigates change in the EU Community includes a vastly improved ICT security infrastructure for future sensitive and valuable computer applications, systems with higher availability, greater survivability from targeted attacks, improved stability during periods of aggressive behaviour by any nation providing a certificate authority.**

⁸⁶ Sheldon, F. T., Abercrombie, R. K., and Mili, A. Methodology for evaluating security controls based on key performance indicators and stakeholder mission. In HICSS '09: Proceedings of the 42nd Hawaii International Conference on System Sciences (Washington, DC, USA, January 2009), IEEE Computer Society, pp. 1–10. Available at <http://www.csm.ornl.gov/~sheldon/public/PID736557-Methodology%20for%20Evaluating%20Security%20Controls%20Based%20on%20Key%20Performance%20Indicators%20and%20Stakeholder%20Mission.pdf>

⁸⁷ Sheldon, F. T., Abercrombie, R. K., and Mili, A. Evaluating security controls based on key performance indicators and stakeholder mission. In IEEE Intelligence and Security Informatics 2009 (2009), vol. June. Slideshow available at: <http://www.isiconference.org/2009/FrederickSheldon.pdf>

Short-Medium Future (Public Key encryption & Quantum Computers)

7. The additional benefits from a report which instigates change in the EU community with respect to quantum computer attacks is:
 - a. **a significant reduction in the amount of intellectual property/sensitive personal data that will be at risk of exposure,**
 - b. **a reduction in the severity of ICT exposure to real-time attacks against access control systems,**
 - c. **the avoidance of “reworking” expensive EU funded critical infrastructure projects from known anticipated attacks, and**
 - d. **improved design and reduced operational costs** by avoiding rip-and-rapidly-replace scenarios that would otherwise occur by non-action today.

With regard to PKI and quantum computing, in our opinion, it is a risky strategy for the EU to aggressively fund codebreaking research and development without adequately preparing for the arrival of these machines. This is particularly the case given quantum computing research has the potential to negatively affect the data security of every European citizen.

We are not suggesting that the fundamental research into quantum computing should be reduced, or slowed, particularly as this is an internationally competitive research agenda. What we are arguing is that there has been insufficient co-ordinated effort by the EU to ensure adequate guidelines are in place and enforced within EU funded research and development programs to address the known risks. The EU call for 50-to-100 year security was displaced and ineffective in inducing change of behaviour.

To our mind it is incomprehensible that the EU has not funded, at least to an equivalent level, the RESEARCH, DESIGN, DEVELOPMENT and DEPLOYMENT of appropriate low-risk countermeasures at the READY to ensure the global community can protect against the negative side-effects of the EU research initiatives in quantum computing.

We assert again that a risk management study on all the known weaknesses of PKI is the first step that will allow the EU community to begin making a comprehensive risk management strategy as a result of deploying and relying on PKI

7.2 Some issues that need to be studied regarding the presence of single point of trust failures rampant throughout modern globally deployed security systems

To the best of our knowledge, there has not been a comprehensive report identifying the security risks to the European community from the known weaknesses in the trust model of PKD systems.

A risk assessment report may consider:

- *) Establishing the extent of dependence on standards based PKI.
- *) The potential impacts of an identity management failure by a PKI vendor
- *) The vulnerability level and potential impact of European Citizens and commercial organisations to International PKI cyberwar by a foreign Root Certificate Authority
- *) A study on the prevalence of insider attacks in the ICT community as a whole, and compare that with the prevalence of insider attacks in the Root Certificate Authority community, and the ability of the providers of PKI infrastructure to adequately mitigate, detect, and repair from insider risks.

7.3 Some issues that need to be studied regarding the impact of quantum computing advances

To the best of our knowledge, there has not been a comprehensive report calculating the full potential impact of the arrival of quantum computing. A risk assessment report may consider:

- *) The costs to the EU community with 10 years data confidentiality of sensitive data
- *) The costs to the EU community with only 5 years data confidentiality
- *) The costs to the EU community with only 1 year data confidentiality
- *) The costs to the EU community in the face of an abrupt loss of all confidentiality
- *) The costs to the EU community if 100% of the identification and authentication systems fail
- *) The costs to the EU community if 50% of the identification and authentication systems fail
- *) The costs to the EU community if 10% of the identification and authentication systems fail
- *) The cost to study the readiness of SKD and PKD countermeasures.
- *) The cost to deploy experimental next generation PKD countermeasures over a 5 year period
- *) The cost to deploy experimental next generation PKD countermeasures over a 1 year period
- *) The cost if the deployed experimental next generation PKD countermeasure fails due to the required globally focussed cryptanalysis finding at catastrophic weakness 5 to 10 years after its full deployment
- *) The cost to develop robust SKD countermeasures, at the ready
- *) The cost to deploy robust SKD countermeasures over a 5 year period
- *) The cost to deploy robust SKD countermeasures over a 1 year period

8. Key Points in Tabular Form

In this section we have numbered 90 issues in the following 8 subjects:

- (6) Single Point of Trust Failure
- (10) Public Key Encryption
- (45) Public Key Infrastructure
- (3) PKI - Liability Shifting
- (2) QKD - Quantum Cryptography
- (9) Cyber Security / Cyber War
- (13) Biometrics
- (2) Panopticon

| Single Point of Trust Failure | | |
|-------------------------------|-------------|--|
| Issue Number | In Sections | Description |
| SPOTF-001 | 5, 6.3.3 | Systems with SPOTF may be sought by countries seek to be a single point of control over all data exchanged to gain advantage over other countries |
| SPOTF-002 | 5, 6.3.3 | Systems with SPOTF may be sought by countries seek to be a single point of control over all data exchanged to oppressively control their citizens and prevent political dissidents |
| SPOTF-003 | 5.1, 6.3.3 | Systems need to be designed to mitigate inappropriate behaviour from occurring, for example through models that offer redundancy and distributed trust, and that enable its detection when it does occur |
| SPOTF-004 | 5.1, 6.3.3 | The majority of fraud is perpetrated by insiders. KPMG’s 2007 “Profile of a Fraudster Survey,” based on actual cases in Europe, the Middle East, and Africa, found that 86 percent of perpetrators in the cases studied held management positions; 60 percent of those were members of senior management or board members. Eleven percent were chief executive officers. |
| SPOTF-005 | 5.1, | “In Germany there is a system where you are not allowed to bribe a civil servant, but you are allowed to bribe a deputy. This is under German Law allowed. And the members of our parliament don’t want to change it. And this is why they cannot sign the U.N. Convention against Foreign bribery. One of the very few countries that is preaching honesty and good governance everywhere in the world, but are not able to ratify the convention.” Self-regulation is difficult. |
| SPOTF-006 | 6.3.6 | <p>We observe that the design of security systems by financial institutions, very large commercial organisations, national institutions or military institutions may be likened to the systems governed by Aristocracies. These systems tend to shift liability and provide advantage and reduced accountability to the most powerful actors.</p> <p>To prevent this, the policies and procedures codified in a security systems architecture must be designed in a balanced way to take into account the legitimate interests of all stake-holders, to ensure accountability for all stake-holders, and prevent liability shifting or the granting of advantage for commercial or national interests.</p> |

| Public Key Encryption | | |
|-----------------------|---------------------------|---|
| Issue Number | In Sections | Description |
| PKE-001 | 5, 6.3.7.2 | The risks of quantum computer attacks against PKE was described as a “nightmare” as early as 2004, with the potential for countless amounts of past and present secure data being exposed and a vast array of critical systems put at operational risk |
| PKE-002 | 5, 5.1, 5.2, 6.1, 6.4.3.2 | NIST has stated “ <i>that in the light of quantum computing CKM system designers MUST look at means other than using public key-based key management systems</i> ”, so that these systems can achieve “ <i>resilience against quantum computing attacks</i> ”. |
| PKE-003 | 5, 6.1, 6.3.7.1 | It is a fact that some internationally recognised quantum computing experts have warned that quantum computers may grow to a size that will catastrophically break all existing deployed public key cryptography, include key exchanges and digital signatures, possibly within 10 years |
| PKE-004 | 5 | PKE is typically deployed in ways where the PKE is a brittle single line of defence that offered no resilience or possibility for recovery. |
| PKE-005 | 5 | The use of at-risk PKI encourages attackers to perform “wait-and-see” attacks in which an attacker archives encrypted ciphertext and waits a short while for the arrival of code-breaking quantum computers become available and then decrypts the archived ciphertext exposing the original content. |
| PKE-006 | 5.1, | A CKM system that meets the requirements raised by NIST during the CKM conference does not exist and needs to be developed. |
| PKE-007 | 5.2, 6.3.7.2 | There has not been significant focus in the cryptographic community to find new public key algorithms that are both classical secure and secure against quantum computers. There has not been sufficient cryptanalysis of existing proposals. This is currently considered an OPEN PROBLEM. |
| PKE-008 | 5.2 | The risk of fast-tracking a competition to pick a new public key algorithm that is both classical and post quantum secure is that this algorithm will not have had sufficient cryptanalysis to build confidence in the algorithm. It may be discovered shortly after that the solution was not secure in practice. |
| PKE-009 | 5.2 | The field of quantum computation is very new and new algorithms are still being developed that may be of reference to candidate. Many classical cryptographers are not aware of the range of existing quantum algorithms. |
| PKE-010 | 5.3, 6.4.4.3 | For every classical security rating, Elliptic Curve Cryptography (ECC) is more vulnerable than RSA/D&H public key algorithms on account of the shorter key lengths in ECC. The quantum computer does not need to have as many ‘qubits’ of memory and the number of quantum operations required is less. ECC may die first. ECC is promoted by the NSA Suite B algorithm for securing Classified International Government Traffic. |

| Public Key Infrastructure | | |
|---------------------------|----------------------|---|
| Issue Number | In Sections | Description |
| PKI-001 | 5, 6.1 | PKI already protects transactions worth trillions and investments worth tens of billions, almost the entire globe is betting the whole shop on PKI |
| PKI-002 | 5, | PKI is a brittle single layer of defence with many known complex problems and limitations |
| PKI-003 | 5, 6.3.8, 6.4.4.3 | The global community knows that fact that Government standards based PKI could catastrophically fail within ten years, but the EU continues massive PKI rollouts even in long term (10-30+ year) critical infrastructure projects |
| PKI-004 | 5, | The extent of PKI dependency and the complexity of the issues/problems and their international scope, relate to and threaten the heart of EU principles, Market future, and stability |
| PKI-005 | 5, 6.1, 6.4.2, 6.4.3 | USA has already started a major project (NIST CKM project) to look for an alternative to public key infrastructure (symmetric key system) |
| PKI-006 | 5, | The issue of finding a replacement to PKI affects all of Europe. |
| PKI-007 | 5, 6.3.6 | A PKI replacement must be balanced so that it takes into account the legitimate interests of all stake holders and does not favour the (political, commercial, military) interests any one nation or group |
| PKI-008 | 5, | A PKI replacement must be internationally acceptable to enable inter-operability of future global ICT systems |
| PKI-009 | 5, | There is a growing massive global reliance upon public key cryptography and the momentum in both Government and commercial deployments continues to build, in spite of the known complex and potentially catastrophic risks and limitations |
| PKI-010 | 5, | When this momentum [PKI-009] and complexity is coupled with the constraints caused by the current harsh economic times, it is obvious that it is not economically viable to research, develop and trial new solutions, even to protect against potentially catastrophic known risks, unless there is already an identified buyer |
| PKI-011 | 5, | For the buyers their reticence to support the development of new solutions is compounded by the already existing problems with interoperability and standards compliance. Consequently designers will not explore alternative approaches. |
| PKI-012 | 5, | The lack of adequate research and analysis on these known risks can trigger a chain of side-stepping and liability shifting |
| PKI-013 | 5 | Europe must co-ordinate with the US efforts or, as we will show, massive fractures in the international markets can occur. |
| PKI-014 | 5, | USA has already started a major project (NIST CKM project) to look for an alternative to public key infrastructure that is resilient to quantum computer attacks |
| PKI-015 | 5.1, | Civilian PKI systems exhibit system-wide (global) single points of trust failure, that permit several parties to create cyber war or to conduct fraud. |
| PKI-016 | 5.1, | In the ICAO Machine Readable Passport scheme, there are over 183 ICAO members, and each ICAO member needs to run their own Root Certificate Authority. If a reader does not have the current certificates for the RCA, it is not possible to validate the integrity of passports from the country. Currently only 17 out of the 183 ICAO members are using a common public key directory. |

| Public Key Infrastructure | | |
|---------------------------|----------------------------|--|
| Issue Number | In Sections | Description |
| PKI-017 | 5.1, | The forgery of RFID MRP has been convincingly demonstrated when the self-signed certificate in the RFID chip is not validated against an external database. |
| PKI-018 | 5.1, | To improve the security of the ICAO MRTD/MRP scheme, the UK NIC uses an online registry to validate that details of the passport. The system does not rely on the passport/id card being cryptographically secure in its own right. |
| PKI-019 | 5.1, | It is difficult to promote new approaches to replace PKI, because at least in the aerospace and defence community it took 5 years just to agree how to implement an existing US Government standard for PKI. |
| PKI-020 | 5.1, | The MD5 Rogue Certificate Authority attack demonstrated that a security weakness in one Root Certificate authority can be exploited to impersonate any website on the Internet, including banking and e-commerce sites secured using the HTTPS protocol. |
| PKI-021 | 5.1, 6.1, 6.3.2 | PKI is only as strong as the weakest root certificate authority, and there are more than 20 different root certificate authorities run by 20 different organisations distributed across the globe. Why was it designed this way? Who gains from this architecture? Who is put at risk by this architecture? |
| PKI-022 | 5.1, | Some prominent root certificate authorities, such as Versign, operate multiple independent root certificate authorities at different levels of quality, with the inside knowledge and comprehension that this behavior weakens the security of the global PKI. |
| PKI-023 | 5.1, | If the existing system wide single point of trust failures inherent in PKI were accurately presented and comprehended to the wider community, would this undermine confidence in eCommerce, and the acceptance of eGovernment initiatives, where the guarantee of authenticity of certificates is critical? |
| PKI-024 | 5.1, | The weakness in the architecture of PKI permits one country to force a Root Certificate Authority operating in its country to conduct cyber-war against other countries. |
| PKI-025 | 5.1, 6.3.2, 6.3.5 | The weakness in the architecture of PKI permits internal fraud to be perpetrated by one RCA against the global community. |
| PKI-026 | 5.1, | Incrementally upgrading the Existing PKI Standards would meet with great resistance from virtually all fronts. |
| PKI-027 | 5.1, | A corrective replacement to PKI must take all known factors into account, and offer a technology and service that is aligned to the welfare of the global community and not just the interests of any one commercial/national organisation |
| PKI-028 | 5.1, | <i>“Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation (of the United States)”</i> fails to take into account legitimate international interests, and fails to mitigate Militarisation, Cyberwar or designs that favour the <i>“National Interests”</i> of one Nation over another Nation. |
| PKI-029 | 5.1, 6.1 | With the massive momentum built up around the deployment of the 20th century security solutions using PKI, at-risk PKI is the main contender to protect all the latest European Government ICT initiatives and major infrastructure projects such as SESARJU. |
| PKI-030 | 5.1, 6.1, 6.4.3.1, 6.4.3.2 | NIST has identified that current PKI can reach to service millions of users. However, new CKM solutions are required to scale several magnitude more in the near future. |

| Public Key Infrastructure | | |
|---------------------------|---------------------|--|
| Issue Number | In Sections | Description |
| PKI-031 | 5.1, | Due to the economic climate and entrenched interests, most security vendors would not be willing to allocate funds to the study and trial of new designs, unless there is strong Government backing. |
| PKI-032 | 5.1, | The magnitude of the issues is beyond the study and reach of any player, even a leading nation. It will be difficult for countries to make the necessary changes, for a globally appropriate system, when national self-interest is in play, and particularly for those countries militarising their cyber interests. |
| PKI-033 | 5.2 | There is institutionalised blindness on the known risks inherent to current PKI standards. |
| PKI-034 | 5.2 | Key length advisors traditionally make recommendations with explicit the explicit proviso that “code-breaking quantum computers do not become a reality in the near future”. The same advisories do not provide adequate advice or alternatives for institutions seeking to address the code-breaking quantum computer threat. |
| PKI-035 | 5.2 | There are no Government standards for public key algorithms that are both classically secure and secure against quantum computers (2010). Searching for such a standard will at the very shortest require 7 years and could require 8 to 10 years. There is no guarantee an acceptable candidate would be found from this competition due to the special properties required by public key cryptography and the future anticipated quantum algorithms. |
| PKI-036 | 5.2, 6.3.7.1, 6.3.8 | The EU, US, and China Governments are funding research into code breaking quantum computers. <i>“The National Security Agency, which supports research in quantum computing, candidly declares that given its interest in keeping U.S. government communications secure, it is loath to see quantum computers built. On the other hand, if they can be built, then it wants to have the first one.”</i> |
| PKI-037 | 5.3 | The design and analysis of a PKI based systems cannot generally be applied to Symmetric Key Infrastructures because they are fundamentally different approaches to the same problem. Money spent developing PKI solutions is wasted if the global community shifts to SKI in the future. |
| PKI-038 | 6.1 | Identity Management is an emerging focal point in both the EU and the US political agendas as a critical component of cyber security that must be improved. Identity management and Cryptographic Key Management are tightly interrelated. Public key cryptography is the dominant technology used in cryptographic key management and identity management today. |
| PKI-039 | 6.3.2 | <i>“Even if [ed: a] compromise [ed: of a certificate authority] is detected in a timely manner, the impacts can be catastrophic to an agency's operations regardless of whether a loss of funds occurs from the compromise.” ... “Should the certification authority be compromised, the agency would have to go through the time consuming and costly process of reissuing digital certificates in accordance with the agency's policies and procedures.”</i> |
| PKI-040 | 6.3.5 | Current PKI based key exchange systems have resulted in a transfer of various difficult responsibilities such as key management to the end user and the complexities involved are a hindrance to the ubiquitous take up of encryption! |

| Public Key Infrastructure | | |
|---------------------------|----------------|--|
| Issue | In Sections | Description |
| PKI-041 | 6.3.5 | Reaching agreement between competing nation states and corporations about whose/which cryptographic algorithms to use creates major obstacles to international collaboration. The fear is that one country may be able to decrypt data from an algorithm that it promotes others to use. |
| PKI-042 | 6.3.5 | Today the retroactive application of (m-1) redundancy in public key infrastructures has limited short-term value because of the known quantum computing threats to all standards based public key cryptography which would put a limited life time on this corrective action. The effort to fix single-point-of-trust problem in an infrastructure that has known catastrophic future risks is not very cost effective. The known mid-to-long term threats are the reason given by the NIST CKM Project Leader Elaine Barker for her call at the NIST CKM Workshop for the study of symmetric solutions that do not rely on PKI. |
| PKI-043 | 6.3.8, 6.4.1.2 | If just one (open or closed) code-breaking quantum computing research project is successful, that group can provide code-breaking and forgery services to Governments, national intelligence organisations, military organisations, or terrorists anywhere in the world. |
| PKI-044 | 7.1 | There are no known approximations of how much each stakeholder stands to lose due to a requirement or component of the system failing on account of the various known risks to PKI. |
| PKI-045 | 7.1 | With regard to PKI and quantum computing, in our opinion, it is a risky strategy for the EU to aggressively fund codebreaking research and development without adequately preparing for the arrival of these machines. This is particularly the case given quantum computing research has the potential to negatively affect the data security of every European citizen. |

| PKI - Liability Shifting | | |
|--------------------------|-------------|--|
| Issue | In Sections | Description |
| PKILS-001 | 5.2 | The scale of the problem with PKI will make it easy for each group to shift liability away from itself. The Standards bodies can say that the cryptographic community had not focussed sufficiently on providing them candidate algorithms. The Cryptographic algorithm designs can argue that there was not sufficient confidence on when quantum computers will arrive, so it wasn't worth their time studying. The organisations implementing cryptography can assert they simply followed Government Standards to the letter and could not be responsible if the standards body didn't provide sufficiently secure algorithms and infrastructure. ... and so on. |
| PKILS-002 | 5.2 | There is the risk that if a comprehensive solution is not designed and proposed BEFORE the urgency of quantum computer attacks becomes critical, the community may be forced to rapidly select a plug-and-play public key alternative of unknown security. This may result in a global replacement of an algorithm that might be no more secure (or even less secure) than the algorithms they replaced. |
| PKILS-003 | 5.3 | Security teams may try to shift the responsibility of making difficult choice between a low-cost risky upgrade to an experimental PKI solution, and a more expensive upgrade to a robust Symmetric Key Infrastructure solution. Given two "short-term secure solutions", one vastly cheaper than the other, investors and management are inclined to go with the cheaper solution. This scenario does not need to be occur if the security issues are addressed now, rather than mid-way through a project. |

| QKD - Quantum Cryptography | | |
|----------------------------|-------------|---|
| Issue Number | In Sections | Description |
| QKD-001 | 5.1 | An attack recently eavesdropped 100% of a quantum cryptographic key due to weakness due to a photon detector vulnerability. |
| QKD-002 | 5.1 | SECOQC advises that current QKD networks are not suitable for use as large scale public networks such as the Internet. |

| Cyber Security / Cyber War | | |
|----------------------------|---------------|--|
| Issue Number | In Sections | Description |
| CYBER-001 | 5, 6.1 | According to the United Nations Telecommunication Chief's warning in 2009 the risk of the next world war being in cyber space. <i>"There is no such thing as a superpower in cyberspace, because every individual is one superpower in itself, because it is the human brain that makes a difference in this field. This is one natural resource that is equally distributed in the world."</i> |
| CYBER-002 | 5.1 | The Internet is becoming increasingly Militarised by Governments. The U.S. Air Force is advocating more Cyber War attacks by American Cyber War organizations. |
| CYBER-003 | | The U.S. has already conducted cyberwar in IRAQ. Attacks exploited the mobile phone network. |
| CYBER-004 | 5.1 | The U.S. Cybersecurity Initiative is primarily to protect .mil and .gov information. Somebody should worry about .com. Ninety eight percent (98%) of the world is .com or .edu or .org or a foreign segment of the global internet. |
| CYBER-005 | 5.1 | What the cost will be to support the necessary research and development, and globally coordinated efforts for that remaining 98%, and what role Governments, United Nations, and the Organisation for Economic Co-operation and Development will play |
| CYBER-006 | 5.1, 6.1, 6.2 | There is new legislation being rapidly advanced in the USA that would require the US NIST to lead the USA's international cybersecurity standards |
| CYBER-007 | 5.1 | New Identity Management and cyberspace security standards may become weapons of coercion and not tools of global social empowerment for the other 98% of the world's population. Without international participation at the highest level, without a system of checks and balances, global identity management issues may not be addressed in a way that is appropriate to the European or global civilian community. |
| CYBER-008 | 5.2 | Fixing security issues after deployment is extremely expensive and may not work comprehensively, such as with the deployment of the Internet. |
| CYBER-009 | 5.2 | When security is not mandatory in ICT systems, cryptography is used as a pricing differential, which results it the bulk of systems not deployed with security. Then we have the situation today, where everyone begins to panic about insecurities which could have been prevented. Panic shifts quickly to offensive militarisation to 'deter' attacks, which leads to cyber war. |

| Biometrics | | |
|-------------------|--------------------|--|
| Issue | In Sections | Description |
| BIO-001 | 5.1, | The set of biometrics captured for the UK Identity card is the same set of biometrics that they capture when enrolling convicted criminals into prison |
| BIO-002 | 5.1, | Do we created a government controlled Panopticon when we combine the biometrics of every citizen with CCTV and other systems? |
| BIO-003 | 5.1, | Biometric data does not change significantly over the life time of an individual, however the cryptographic mechanisms to protect biometrics are not rated for 100 year security. |
| BIO-004 | 5.1, | Algorithms that are known to be at risk of catastrophic security failure after 10 years are used to protect biometrics. |
| BIO-005 | 5.1, | The United States is trading biometrics with other countries. According to one source, approximately 25 countries have bilateral biometric trading agreements in place with the United States. |
| BIO-006 | 5.1, | India has explicitly declared it wants to capture the biometrics of every citizen. The UK appears to be going in this direction with the National Identity Card program. |
| BIO-007 | 5.1, | The United States captures the biometrics of everyone entering the country. |
| BIO-008 | 5.1, | EU citizens are having their biometrics permanently captured and used or passed on in ways that they can not audit, or control. EU Citizens have lost self-determination over their captured biometrics. |
| BIO-009 | 5.1, | Biometric data may be used in identity fraud attacks. |
| BIO-010 | 5.1, | Biometric data is being managed by Government systems and Government approved protocols. These systems are using brittle cryptographic protections that are vulnerable to single point of trust failures. Furthermore, Governments have a bad track record of protecting sensitive data. |
| BIO-011 | 5.1, | Newly acquired biometric information can be used to retro-actively track an individual. |
| BIO-012 | 5.1, | Biometric enabled passports and ID cards may need to be valid for 10 years, even though the security of the cryptography in that document may fail within that time due to code breaking quantum computer attacks. |
| BIO-013 | 5.1, | PKI encrypted biometrics may be exploited within the life-time of their owner, even if those biometrics are later encrypted using stronger cryptography. |

| Panopticon | | |
|-------------------|--------------------|--|
| Issue | In Sections | Description |
| PAN-001 | 5.1 | The definition of “a dangerous person”, or “terrorist”, is very flexible and open to different political interpretation. |
| PAN-002 | 5.1 | By correlating mobile phone cell data in combination with extensive CCTV networks and facial recognition systems supplied with civilian biometric data, it may not be possible, in the near term future, for anyone to move outdoors in city areas with any privacy from Governments |