SYNAPTIC
LABORATORIES LTD.

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

Monday, 13 September 2010

To: **The National Telecommunications and Information Administration** at
U.S. Department of Commerce, 1401
Constitution Avenue, NW., Room 4725,
Washington, DC 20230.

Re: **Cybersecurity, Innovation and the Internet Economy**
Notice of Inquiry

This letter is written in response to the notice for inquiry made in the [Federal Register: July 28, 2010 (Volume 75, Number 144)], [Page 44216-44223], [Docket No. fr28jy10-39].

Thank you for making this important call for public comment.

We have selected questions out of your notice of inquiry which we have provided answers to.

> *"Comments containing references, studies, research, and other empirical data **that are not widely published** should include copies of the referenced materials."*
>
> *Cyberspace, Innovation and The Internet Economy*

In consideration of the text above, we will avoid submitting copies of publications that can readily downloaded from the Internet. We request that all citations found in this document be considered as part of this submission.

Yours sincerely,

Benjamin Gittins

Chief Technical Officer
Synaptic Laboratories Limited
September 13, 2010

Before providing Synaptic Labs' input, I would like to provide some context.

Synaptic Laboratories is a micro Private Technology Company managed by Australian citizens with Directors in Gozo, Malta (Europe) and Australia. We are operating internationally on a 'virtual' basis with ten years of completed cross domain research and design. Our core business is cutting edge cyber security solutions for Today's Internet (and the Future Internet).

We are active in the US Federal Cybersecurity initiatives:

- having made submissions to the NITRD Cyber Leap year public Requests for Input[1]
- having participated at the 'by invitation' NITRD Cyber Leap Year Summit where 6 of our proposals were carried forward in the Participants Ideas Report[2]
- having presented further information on these proposals[3] at the peer reviewed Oak Ridge National Laboratory 6th Annual Cyber Security and Information Intelligence Workshop (CSIIRW)[4] held in April 2010 and also at the IEEE Key Management Summit held in May 2010, where we were a sponsor[5].
- having provided 157 pages of detailed technical feedback to the NIST Cryptographic Key Management project in August 2010.

Specifically Synaptic Labs is focussing on Global-scale Identity Management and Cryptographic Key Management (IdM/CKM) along the lines called for by the U.S. Department of Homeland Security in their Nov. 2009 "*A Roadmap for Cybersecurity Research*" publication[6], and on next generation Internet protocols with privacy enhancing features as published in the NITRD NCLY 2009 Participants Report[7].

Synaptic Labs was one of the few foreign participants invited to the NITRD National Cyber Leap Year Summit.

Synaptic Labs has been acting as a bridge between US and European Government Level security initiatives, seeking to bring to the attention of the other overlapping initiatives where synchronisation and international normalisation may be possible.

---

[1] http://synaptic-labs.com/resources/synaptic-publications/104-input-to-ec-and-us-funded-ict-initiatives/348-pub-synaptic-labs-3-inputs-to-nitrds-call-for-qleap-aheadq-ideas-2009.html

[2] http://synaptic-labs.com/resources/security-bibliography/105-security-organisations-projects-and-calls/331-bibliography-us-nitrd-ncly-security-summit-2009.html

[3] http://synaptic-labs.com/resources/security-bibliography/106-security-conferences/340-bibliography-us-ornl-csiirw-6-2010.html

[4] http://www.csiir.ornl.gov/csiirw/10/index.html

[5] http://2010.keymanagementsummit.org/ and http://storageconference.org/2010/Presentations.html#KMS

[6] http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[7] See our extracts from this report here: http://media.pqs.io/pub/papers/NCLY/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf

RFC 1. Quantifying the Economic Impact

With regard to quantifying Economic impact we copy in full Synaptic Laboratories two proposals submitted into and accepted for publication by the NITRD in their NCLY Summit 2009 – Participants' Ideas Report as possible suggestions for studies relevant to your questions[8]:

6.1 Idea - Evaluating the Effectiveness of Data Depersonalization Techniques and It's Impact on the Community

6.4.1 Description

Establish if data depersonalization techniques used by the civilian industry are effective and assess the impacts of re-sale of depersonalized data in the community. Study the way consumers of depersonalized data use the information. If the depersonalization techniques are not adequate to protect identity (before or after sale), identify what techniques and parameters are appropriate for commercial data depersonalization. After adequate peer review, enforce these techniques and parameters as Government policies.

6.4.2 Inertia

Commercial interests for selling data / Poor community-wide awareness of the risks associated with sale of personal data collected by organizations.

6.4.3 Progress

Several papers have identified that it is possible to identify the persons present in some depersonalized data released by large organizations.

6.4.4 Action Plan

Identify the security and legal experts / acquire large representative data sets of the type of information sold / start a conference and advance it with funding.

Who can help:

NITRD, US State Department, Electronic Freedom Foundation, Jeff Jonas of IBM, weak signal analysis, other published researches in this field.

6.4.5 Jumpstart Activities

Collect a large representative sample of commercial exchanged depersonalized data (find data sold by a large online commercial store, and a mobile phone provider selling location data), bring together experts in the field to evaluate how easy it is to re-personalize the data, bring together legal team to evaluate the implications of data that is not effectively disassociated from the user. Compile any changes required to law.

6.5 Idea - Measuring the Impacts of Unauthorized Information Disclosure

6.5.1 Description

Methodologies for evaluating appropriate security controls based on the confidentiality, integrity and availability of IT systems now exist. However insufficient information exists to allow an organization to establish the value of information loss to stakeholders, including customers and clients. **Without such information it is not possible to make an informed decision about the necessary level of security mechanisms required.** Large scale field studies are required to establish the value of information loss with respect to different classes of data including financial, medical, intellectual property, relationship information and geolocation of time for different groups including Enterprises, SME, and individuals. Such studies could be extended to assess the financial and emotional impact of down-time or availability of access to services. **A greater understanding of the value of information managed by others, and its management, by the stake holders can better inform organizations on how to manage their IT infrastructure and risks.**

6.5.2 Inertia

Commercial interests for selling data / Commercial interests to maintain 'just-enough' security to protect against legal liability. There is little incentive for organizations to identify the true cost of security breaches against individuals.

6.5.3 Progress

Technologies exist which can be used to collect this information.

6.5.4 Action Plan

Identify interested financial, social sciences, security and legal experts. Develop action plan and secure funding. Perform studies in hospitals and other medical practices.

Who can help:

NITRD, CyberSpace Sciences and Information Intelligence Research - ORNL - DOE, RTI International, US Universities, EU Think Trust.

6.5.5 Jumpstart Activities

Identify the financial, social sciences, security and legal experts. Develop a set of questions to measure metrics on. Engage many universities and some organizations to perform surveys and collect the data.

---

[8] QinetiQ. National Cyber Leap Year Summit 2009 – Participants' Ideas Report. On behalf of the US NITRD Program. Available at http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Participants_Ideas_Report.pdf

RFC 2. Raising Awareness

One suggestion is that on installation of an operating system (Linux, Windows, OS X) the vendor could offer the user the opportunity to open up a web-page / short video that provides basic education on Internet Security and where Civilian's can go to access regional cybersecurity authorities. For example several countries could work together to produce a multi-lingual service that pointed people to their local authorities. In addition to raising awareness of where to report cybercrime, civilians and businesses may be more willing to report the crime if they perceive their disclosure will genuinely result in tangible improvement in security for themselves or others.

RFC 3. Web Site and Component Security

We propose that operating systems vendors could be encouraged to provide much-greater situational awareness to power-users/administrators. It should be possible for *any* user to see detailed breakdown of network activity, file access, configuration access, and so on... of any application running on their computer without purchasing additional software. This way the community at large can gain greater understanding of how programs are behaving and notify others if something inappropriate is identified.

RFC 4. Authentication/Identity (ID) Management

This section is subdivided into several sub-sections RFC 4.1, RFC 4.2, and so on.

RFC 4.1

> *"The Department seeks comment on the effectiveness of current identity management systems in addressing cybersecurity risks."*
>
> *Cyberspace, Innovation and The Internet Economy*

It is widely felt in the global cryptographic community that the current **civilian** X.509 identity management system is in a state of disarray. We strongly recommend studying Peter Gutmann's comprehensive book "Engineering Security" (Dec. 2009)[9]. It provides the most comprehensive analysis on the security problems found in today's public key infrastructure and identity management systems. We have extracted several important problems and summarised them in the following document[10].

To provide supporting evidence regarding the negative public opinion in the American cryptographic key management community with regard to the civilian public key infrastructure we quote in full a short blog discussion[11] between Luther Martin (Chief Security Architect of Voltage Security, on the program committee of IEEE KMS 2010), Peter Gutmann (PKI expert, Department of Computer Science at University of Auckland), and myself:

> **Is PKI really that bad?** (Tuesday, 01 June 2010)
>
> **Luther Martin:**
>
> At the recent **IEEE** Key Management Summit[12], we scheduled a few minutes at the end of each day so that people could get up and talk about whatever issues they felt like talking about. The intent was to provide a way for people to tell the others about ideas that they had had while listening to the various speakers' presentations. I had never seen this done before, but it seemed to work fairly well.

---

[9] Available at http://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf

[10] Gittins, B., and Kelson, R. "A detailed look at the positive and negative security aspects of today's X.509 Civilian Public Key Infrastructure". Slideshow, Synaptic Laboratories Limited. www.synaptic-labs.com/resources/streaming-videos/sll-cybersecurity-series.html#problems_pki

[11] http://superconductor.voltage.com/2010/06/is-pki-really-that-bad.html

[12] http://2010.keymanagementsummit.org/

The impromptu session at the end of the second day was particularly interesting. One of the attendees, Ben Gittins, got and asked[13] for opinions on what he had read about PKI. Peter Gutmann, for example, is now working on a new book, and Ben had read a preliminary version of this book's chapter on PKI. Apparently Peter's new book does not describe PKI in a positive way (if you're familiar with Peter's thoughts on PKI, you'll know that that's a huge understatement), and Ben wanted to know if we really thought that PKI was as bad as Peter describes it to be.

It didn't take long for the group to reach a consensus. A few people simply said, "Yes, it really is." That's about as far as the discussion got. After that, there really wasn't much more to say.

Peter Gutmann:

One of the reasons for going into so much detail about PKI's problems in the book is that, as the audience members pointed out, people are aware that PKI has major problems but apart from Schneier and Ellison's "Ten Risks of PKI"[14] from 10-odd years ago there doesn't seem to be anything around that documents why. My intent was to answer the implied question "*We're having a lot of trouble with PKI, what are we doing wrong?*" with "***You're not doing anything wrong, it just doesn't work very well***". I guess my real issue with PKI is why, after 30 years of failure to launch, we're still bothering with it instead of looking for alternatives that do work. Now I've got to figure out how to get a ref to this post into the book :-).

Benjamin Gittins:

As for the problems with PKI, Peter's book [1] definitely goes into more detail than any other publication I have found on the "why". It is a real eye-opener and the case-studies drive the issues home.

Thankfully, others are also starting to raise the flag around the civilian PKI. Richard Brooks recently wrote an extended abstract [2] highlighting some of the recent problems at ORNL CSIIRW-6 [3].

While not as authoritative as Gutmann or Brooks there is also a short article [4] published by Network World which touches on the existence of multiple system-wide single point of trust failures (SPOTF) in the civilian identity management system. It points to interception devices sold to exploit this weakness. I also recently posted [5] on the issue of SPOTF as it relates to the US draft (2010) National Strategy for Trusted Identities in Cyberspace publication [6].

Picking up on Peter's comment above "*I guess my real issue with PKI is why, after 30 years of failure to launch, we're still bothering with it instead of looking for alternatives that do work*", I note there are new calls (2009-2010) from US Department of Homeland Security (DHS) and US National Institute of Standards and Technologies (NIST) for new trustworthy global-scale identity management (IdM) [7] and global-scale cryptographic key management (CKM) [8][9] solutions respectively.

Elaine Barker (project leader of the NIST [global-scale] CKM project [8]) stated CKM designers "*must look at means other than public key-based key management schemes; they must look at quantum computing-resistant algorithms and schemes*" [9] (page 31 and page 52).

The DHS cybersecurity roadmap [7] states that: "*Global-scale identity management is a hard problem for a number of reasons, including standardization, scale, churn, time criticality, mitigation*

---

[13] See: 42 minutes 54 seconds into the video "*A new global IdM/CKM design that does not rely on PKC - SLL's response to NIST's call*" for the audio/visual recording of the full discussion held at IEEE KMS on this issue. Find that video at bottom of this page: http://storageconference.org/2010/Presentations/KMS/Videos-SD.html

[14] http://www.schneier.com/paper-pki.html

of insider threats, and the prospect of threats such as quantum computing to existing cryptographic underpinnings." (page 55)

Unfortunately the (DHS led) National Strategy for Trusted Identities in Cyberspace project does not seem to attempt to encompass the hard problems and critical issues identified by the DHS roadmap or take into consideration NIST's efforts. Furthermore, the DHS IdM and NIST CKM initiatives do not appear to be synchronised yet. In my opinion, a harmonisation of these 3 efforts could be beneficial.

Personally I'd like to see the international collaborative development and deployment of an internationally acceptable global scale IdM/CKM architecture that synergistically combines the best of both the public key and symmetric key techniques to address the issues identified by NIST and DHS while also taking into account the many lessons learnt by industry and Government (both in what doesn't work, and what is working in the market today).

I feel it is critical that such an effort provide a upgrade path for existing cybersecurity systems while also framing the global scale IdM/CKM effort in the wider context of how it supports other cybersecurity initiatives such as behavioural trust, various malware detection methods, physical identification techniques, privacy enhancing techniques, anonymity techniques, and so on. Such a system should be explicitly designed to protect the legitimate interests of all stake-holders.

References:

[1] Dr. Peter Gutmann's "Engineering Security", http://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf

[2] Prof. Richard Brooks: "Lies and the Lying Liars that Tell Them - A fair and balanced look at TLS", CSIIRW-6 2010 [proceedings to published by the ACM].

[3] 6th Annual Cyber Security and Information Intelligence Research Workshop held at Oak Ridge National Laboratory, http://www.ioc.ornl.gov/csiirw/10/index.html, http://www.ioc.ornl.gov/csiirw/10/csiirw-schedule-complete.pdf

[4] Ms. Smith, "Certified Lies: Big Brother In Your Browser", Network World, http://www.networkworld.com/community/node/64074

[5] B. Gittins, "We need to explore new distributed decentralised trust models that remove the current system-wide single point of trust failure", NSTIC @ Ideascale, http://www.nstic.ideascale.com/a/dtd/We-need-to-explore-new-distributed-decentralised-trust-models-that-remove-the-current-system-wide-single-point-of-trust-failure-/49483-9351

[6] DHS and others, "Draft - National Strategy for Trusted Identities in Cyberspace", http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

[7] DHS, "A roadmap for cybersecurity research", November 2009, http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[8] NIST, "Cryptographic Key Management Project", 2009, http://csrc.nist.gov/groups/ST/key_mgmt/

[9] NIST, "Final version of the NIST Internal Report 7609", NISTIR-7609, 2009, http://csrc.nist.gov/publications/nistir/ir7609/nistir-7609.pdf

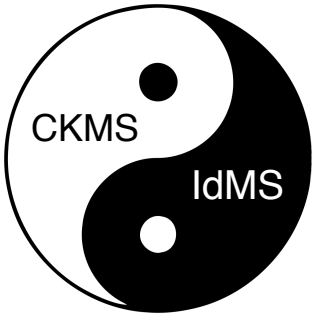
[10] B. Gittins, "NSTIC relies on cryptographic primitives known to be at risk of catastrophically breaking", NSTIC @ Ideascale, http://www.nstic.ideascale.com/a/dtd/NSTIC-relies-on-cryptographic-primitives-known-to-be-at-risk-of-catastrophically-breaking/53072-9351

RFC 4.2

> *"Beyond the measures recommended in the National Strategy for Trusted Identities in Cyberspace, what, if any, federal government support is needed to improve authentication/ identity management controls, mechanisms, and supporting infrastructures?"*
>
> *Cyberspace, Innovation and The Internet Economy*

In our opinion, the National Strategy for Trusted Identities in Cyberspace unfortunately does not go far enough to address known problems with the existing Identity Management Infrastructure that would undermine it's trustworthiness. Specifically in [5] we outline how NSTIC needs to employ a distributed decentralised trust models that remove the current system-wide single point of trust failure and [10] highlights that NSTIC relies on asymmetric cryptographic primitives known to be at risk of catastrophically breaking. Other known issues that we recommend should be addressed within the scope of the NSTIC Identity management vision is that it is not possible to achieve trust when the underlying components/computers are compromised[15]. Another explicit self-imposed limitation in the NSTIC draft is that physical identification was considered outside the scope of their initiative. The following posts stress that others also feel this is not adequate: [16], [17] and [18].

These postings all stress how it is **not** possible to solve cybersecurity problems by narrowing a project's focus down to one-aspect of cybersecurity taken in isolation. To draw out this point further, let us consider two related US Federal Cybersecurity initiatives: The DHS 2009 call for global-scale identity management[19] and the NIST 2009 call for [global scale] cryptographic key management[20].



The New Oxford American Dictionary defines a secret as "*something that is kept or meant to be kept unknown or unseen by others*". Cryptographic systems employ a) to manage keys and establish authenticated private channels and b) Identity Management System to identify and authenticate identities. Electronic Identity Management System use cryptography to authenticate identities and physical Identity Management System to identify people. We can't define an electronic-Identity Management System without defining a Cryptographic Key Management System and vice versa. Identity Management System and Cryptographic Key Management System are as interdependent as Yin and Yang.

That said, unfortunately the NIST 2009 "Roadmap for cybersecurity research" does not mention cryptographic key management in the context of identity management and the NIST Special Publication (SP) 800-130, A Framework for Designing Cryptographic Key Management Systems published in June 2010[21] a total of **8 lines** out of **88 pages** of text was dedicated to identity management. Clearly the design of global-scale cryptographic systems require collaboration between CKM, electronic IdM and physical IdM specialists.

See Synaptic Lab's feedback[22] to NIST's SP 800-130 draft for more information on limitations with the NSTIC process with regard to trustworthiness as defined in the above mentioned roadmap by DHS.

---

[15] http://www.nstic.ideascale.com/a/dtd/There-is-no-possible-trust-when-computers-are-compromised/45311-9351

[16] http://www.nstic.ideascale.com/a/dtd/Flawed-without-reliable-offline-authentication-of-subjects/45766-9351

[17] http://www.nstic.ideascale.com/a/dtd/Concept-of-Identity-is-needed----Seperate-Identity-from-rights-and-privileges./45765-9351

[18] http://www.nstic.ideascale.com/a/dtd/Trusted-identity-is-not-the-same-thing-as-trustworthiness/45954-9351

[19] DHS, "A roadmap for cybersecurity research", November 2009, http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[20] http://csrc.nist.gov/groups/ST/key_mgmt/

[21] Barker, E., Branstad, D., Chokhani, S., and Smid, M. A Framework for Designing Cryptographic Key Management Systems. (Draft) Special Publication 800-130, National Institute of Standards and Technology, June 2010. Available at http://csrc.nist.gov/publications/drafts/800-130/draft-sp800-130_june2010.pdf

[22] http://media.synaptic-labs.com/downloads/pub/publications/NIST/20100816-SLL-NIST-SP800-130-Feedback.zip

RFC 4.3

> *"Do the authentication and/or identity management controls employed by commercial organizations or business sectors, in general, provide adequate assurance? If not, what improvements are needed? What specific controls and mechanisms should be implemented?"*
>
> *Cyberspace, Innovation and The Internet Economy*

No, as outlined above, it is widely felt that the current controls do not provide adequate assurance.

See B. Gittins, "We need to explore new distributed decentralised trust models that remove the current system-wide single point of trust failure", NSTIC @ Ideascale, http://www.nstic.ideascale.com/a/dtd/We-need-to-explore-new-distributed-decentralised-trust-models-that-remove-the-current-system-wide-single-point-of-trust-failure-/49483-9351

See also Gittins, B., and Kelson, R. "A detailed look at the positive and negative security aspects of today's X. 509 Civilian Public Key Infrastructure". Slideshow, Synaptic Laboratories Limited. www.synaptic-labs.com/resources/streaming-videos/sll-cybersecurity-series.html#problems_pki

RFC 4.4

> *"Are the basic infrastructures that underlie the recommended controls and mechanisms already in place? What, if any, new tools or technologies for authentication or identify management are available or are being developed that may address these needs?"*
>
> *Cyberspace, Innovation and The Internet Economy*

In our assessment, the basic infrastructures is NOT in place to enable high-assurance trustworthy global-scale identity management in the civilian community.

This is similar to the published opinion of the U.S. Department of Homeland Security in their call for a trustworthy solution.

Global-scale Identity Management is a US Department of Homeland Security (DHS) cyber-security initiative. This call appears to have originated in the 2005 report[23] by the INFOSEC Research Council Hard Problem List. The associate director for NITRD in 2006 recognised the call for global-scale identity management[24]. It has since carried through to the DHS Roadmap for Cybersecurity Research in Nov 2009[25].

The U.S. Government Accountability Office (GAO) recently produced a document[26] titled: "*CYBERSECURITY: Key Challenges Need to Be Addressed to Improve Research and Development*". In that document they mention: "***global-scale identity management**, which **was identified by DHS as a top problem that needs to be addressed***".

The latest call for global-scale identity management (2009) is framed within a wider context of eleven "Current Hard Problems", many of which hard problems need to be concurrently addressed to achieve a **trustworthy** global-scale IdMS.

---

[23] INFOSEC Research Council, "Hard Problem List", Nov 2005, http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf

[24] Sally E. Howe, "Remarks to the HCSS-Sponsored National Workshop on Beyond SCADA: Networked Embedded Control National Workshop on Beyond SCADA: Networked Embedded Control for Cyber Physical Systems for Cyber Physical Systems: Workshop Deliverables: Roadmap, Hard Problems, and Report", NITRD

[25] DHS, "A Roadmap for Cybersecurity Research", Nov. 2009. http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[26] GAO. "CYBERSECURITY: Key Challenges Need to Be Addressed to Improve Research and Development", GAO-10-466, United States Government Accountability Office, June 2010. Available at http://www.gao.gov/products/GAO-10-466

RFC 4.5

> *"How can the U.S. Government best support improvement of authentication/identity management controls, mechanisms, and supporting infrastructures?"*
>
> *Cyberspace, Innovation and The Internet Economy*

We recommend bringing together the U.S. NITRD, U.S. NSTIC, U.S. DHS global-scale IdMS project, U.S. NIST CKM Project, U.S. NIST Identity Management Systems Research & Development Project, E.U. STORK, China, Russia, and the international commercial sector together to comprehensively build a global-scale cryptographic key management and identity management system hosted in the cloud to protect and uphold the legitimate interests of all stakeholders globally. See Section 4 of Synaptic Laboratories feedback[27] to NIST's SP 800-130 draft for more information on how various current U.S. Cybersecurity initiatives could potentially work together as part of a co-ordinated initiative.

RFC 4.6

> *"Is there a continuing need for limited revelation identity systems, or even anonymous identity processes and credentials? If so, what would be the potential benefits of wide-scale adoption of limited revelation identity systems or anonymous credentialing from a cybersecurity perspective? What would be the drawbacks?"*
>
> *Cyberspace, Innovation and The Internet Economy*

Yes. There are strong arguments in support of both pseudo-anonymity and true non-revocable anonymity. In 2009 the U.S. President's cyberspace policy review[28] near term action plan called for game-changing technologies that have the potential to enhance the security, reliability and **trustworthiness** of digital infrastructure and to build a cybersecurity-based identity-based vision that addresses **privacy and civil liberties interests.** And we quote: *"Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging **privacy-enhancing technologies** for the Nation."*

> *Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by **eliminating or minimising personal data** thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system.*
>
> *van Blarkom, Borking & Olk [29]*

In November 2009 the U.S. DHS enumerated eight current hard problems which "were selected as the hardest and most critical challenges that must be addressed by the INFOSEC research if **trustworthy systems envisioned by the U.S. Government are to be built.**"[30]

These 8 are as follows:

1. Global Scale Identity Management
2. Insider Threats
3. Availability of Time-Critical Systems
4. Building Scalable Secure Systems
5. Situational Understanding and Attack Attribution
6. Information Provenance
7. **Security with Privacy (Privacy aware security)**
8. Enterprise-Level security metrics.

---

[27] http://media.synaptic-labs.com/downloads/pub/publications/NIST/20100816-SLL-NIST-SP800-130-Feedback.zip

[28] USOWH. Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure (May 26, 2009). US, Office of the White House. www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[29] van Blarkom, G.W.; Borking, J.J.; Olk, J.G.E. (2003). "PET". Handbook of Privacy and Privacy-Enhancing Technologies. (The Case of Intelligent Software Agents). ISBN 90-74087-33-7.

[30] DHS, "A Roadmap for Cybersecurity Research", Nov. 2009. http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

Given the U.S. and E.U. share many common sensibilities, let us briefly consider privacy and civil liberties as formally defined from within a EU context.

> *The European citizen's requirements, therefore, are mainly focused around an individual, personal perception of security and dependability and all its related implications. Individual, personal, democratic, self-determined control is much more important to citizens than the traditional, historic, government-controlled central approach to security and dependability.*
>
> ***In the European Information Society, security and dependability concepts must take into account not only central control requirements but also the individual need for security and dependability mechanisms that protect the citizens' privacy and identity.***
>
> *A research framework should pay special attention to areas of security and dependability that do not follow 20th century central command and control approaches, but that instead could lead to an open and trustworthy European Information Society in which the* ***end user is empowered to determine his or her own security and dependability requirements and preferences****. This need for self-determination is accompanied by a need for a reliable, dependable infrastructure that such self-determination can be applied to. Processes of the Information Society will be digitized more and more and there needs to be a reliable, failsafe communications environment and infrastructure in place to support these processes.* [31]
>
> *2.2 The Citizen's Perspectives on Security and Dependability, Deliverable 3.0, SecurIST EU-FP6-004547*

> *Privacy: in the European Union, privacy is generally defined as a right of self-determination, namely,* ***the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others.***
>
> *Regulation addressing this is such as:*
>
> *• European Data Protection Directive that is rooted in the concept of consent, while*
>
> *• California SB 1386 is putting a price tag on privacy*
>
> *Glossary, SecurIST EU-FP6-004547*

See also Sullivan's white paper "On the anonymity 'versus' accountability debate", Think-Trust EU-FP7-216890, June 2010. Available at http://www.future-internet.eu/fileadmin/news/Accountability_vs_anonymity.pdf .

We wish to also stress that non-revocable anonymous publication has historically played an important role in promoting democratic principles.

The Spirit of the Laws (French: L'esprit des lois) is a treatise on political theory first published anonymously by Charles de Secondat, Baron de Montesquieu in 1748 with the help of Claudine Guérin de Tencin. **Originally published anonymously partly because Montesquieu's works were subject to censorship**, its influence outside of France was aided by its rapid translation into other languages.

Montesquieu was the most frequently quoted authority on government and politics in colonial pre-revolutionary British America, **cited more by the American founders than any source except for the Bible**[32]. Montesquieu advocated constitutionalism, the separation of powers, checks and balances, the preservation of civil liberties, and the rule of law with the objective to reduce citizens fear of the political system.

---

[31] SecurIST Advisory Board. Recommendations for a Security and Dependability Research Framework: from Security and Dependability by Central Command and Control to Security and Dependability by Empowerment. Deliverable 3.0, SecurIST EU-FP6-004547, Jan. 2007. http://www.securitytaskforce.eu/dmdocuments/securist_ab_recommendations_issue_v3_0.pdf

[32] Lutz, D. S. The Relative Influence of European Writers on Late Eighteenth-Century American Political Thought. vol. 78, No. 1 of The American Political Science Review, pp. 189–197. Available at http://www.jstor.org/stable/1961257.

RFC 4.7

> *How might government procurement activities best promote development of a market for more effective authentication tools for use by government agencies and commercial entities?*
>
> *Cyberspace, Innovation and The Internet Economy*

The U.S. government procurement processes could require identity management and cryptographic key management systems to systematically and comprehensively addresses the 11 problems that need to be solved to achieve trustworthiness as defined by the U.S. DHS in their "A roadmap for cybersecurity research", November 2009, http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

RFC 4.8

> *Could a private marketplace for ``identity brokers'' (i.e., organizations that can be trusted to establish identity databases and issue identity credentials adequate for authorizing financial transactions and accessing private sector components of critical infrastructures) fulfill this need effectively?*
>
> *Cyberspace, Innovation and The Internet Economy*

Probably not using mainstream X.509 federated PKI technologies as they suffer from a multitude of single point of trust failures. See "*We need to explore new distributed decentralised trust models that remove the current system-wide single point of trust failure*", NSTIC @ Ideascale, http://www.nstic.ideascale.com/a/dtd/We-need-to-explore-new-distributed-decentralised-trust-models-that-remove-the-current-system-wide-single-point-of-trust-failure-/49483-9351

RFC 4.9

> *Should the government establish a program to support the development of technical standards, metrology, test beds, and conformance criteria to take into account user concerns such as how to: (1) Improve interoperability; (2) strengthen authentication methods; (3) improve privacy protection through authentication and security protocols; and (4) improve the usability of identity management systems?*
>
> *Cyberspace, Innovation and The Internet Economy*

The US NSTIC project, with it's focus on interoperability, is probably the **right** forum to address the requirement for increased compatibility and relaxed access controls for only certain parties/components within a CKMS during times of crisis as called for by NSA below:

> *NSA would like to have some interoperability among high-assurance government devices and commercial off-the-shelf devices, especially for emergency situations, such as 9/11 and hurricane Katrina.*
>
> *...*
>
> *NSA wants to support wider audiences of users, including FEMA, allies, charities, State governments, and emergency first-responders.*
>
> *Cryptographic Key Management Workshop Summary, NIST Interagency Report 7609*

The US NSTIC project could also focus on interoperability with the E.U. STORK EU ID project[33].

However, interoperability of today's identity management systems is **not sufficient** to achieve trustworthy global-scale identity management as envisioned by the U.S. Department of Homeland Security. That is, a better co-ordinated identity management ecosystem built on insecure components remains inherently insecure and cannot achieve trustworthiness.

The interoperability results from U.S. NSTIC could be fed as input into the US DHS Global-scale identity management project. Furthermore the DHS global-scale identity management project could be co-ordinated closely with the US NIST [global scale] CKM project as previously recommended.

---

[33] https://www.eid-stork.eu/

RFC 4.10

What are the privacy issues raised by identity management systems and how should those issues be addressed?

Cyberspace, Innovation and The Internet Economy

We recommend that the privacy issues around identity management systems be framed within the context of achieving trustworthiness with respect to the legitimate interests of all stake-holders.

*It's not about security, its about **Trustworthiness** of digital infrastructure.*
Security, Reliability, Resiliance, Privacy, Useability.
...
Say "NO!" to Business as Usual. We don't want it, we can't take it anymore.

Dr. Jeanette Wing,
Assistant director for computer & information science and engineering (CISE), NSF (2010)

To paraphrase Montesquieu, a global-scale IdM-CKM should be set up so no stake-holder need be afraid of another. This requires a conceptual shift away from the `us vs. them' adversarial model inherited from the military origins of cryptography and towards an inclusive regulative system between peers.

Current Government policy/initiatives (Federal PKI, TSCP) tends to push towards silo's of centralised command and control that are not appropriate for use between collaborating peers who each have security obligations in their own jurisdictions. The end result as present today in the civilian X.509 PKI is that collaborators security races to the lowest common denominator which exposes all parties to security failure in any one of the participating jurisdictions.

We assert that principles and requirements outlined by various US Cybersecurity Initiatives (US DHS Trustworthiness, NIST CKM, ...) can be embodied and realised today in a unified trustworthy and cost-effective IdM-CKM system.

A system that enhances democratic principles and protects the legitimate and diversified interests of all stake holders/users, even in a global context of competing nation-states.

In our presentations ([34], [35], [36]) Synaptic Labs' outlines the core architecture of a global-scale platform that can be extended to comprehensively address international CKM, electronic-IDM and physical-IDM in a co-ordinated but distributed, decentralised and diversified manner. Our proposal exploits diversity in membership to improve security through a system of checks-and-balances and separation of powers in a way that ensures the system remains highly available and robust to all stake holders. Diversity used in this manner also encourages international competition in the open market place.

---

[34] Gittins, B. Overview of SLL's proposal in response to NIST's call for new global IdM/CKM designs without Public Keys. In Proceedings of 6th Annual Workshop on Cyber Security and Information Intelligence Research (Apr. 2010), ACM. To appear.

[35] Gittins, B., and Kelson, R. Overview of SLL's proposal in response to NIST's call for new global IdM/CKM designs without PKC. Video. In IEEE Key Management Summit 2010 website (Lake Tahoe, Nevada on May 4-5, 2010., May 2010), IEEE. Available at http://www.synaptic-labs.com/resources/streaming-videos/sll-cybersecurity-series.html

[36] Gittins, B., and Kelson, R. Synaptic Labs' standalone globally scalable Identity and Key Managent Cybersecurity Model addresses some of the current "hard problems in INFOSEC" identified by the USA Department of Homeland Security, and is designed to protect the users of public key cryptography, creating a layered defence with distributed trust. Slideshow and video, Synaptic Laboratories Limited, July 2010. Available at http://www.synaptic-labs.com/resources/streaming-videos/sll-cybersecurity-series.html#layered_defence

RFC 4.11

Are there particular privacy and civil liberties questions raised by government involvement in identity management system design and/or operations?

Cyberspace, Innovation and The Internet Economy

It is not clear if there is a significant improvement in client/stake-holder privacy by avoiding government participating as service providers if some Government's (local or foreign) have overt/covert "legalised" interception capabilities and can retrieve all civilian identity management transaction metadata.

> *On July 12, officials from India's Department of Telecommunications met with representatives of three telecom service provider groups to discuss interception and monitoring of encrypted communications by security agencies.*
>
> *"There was consensus that there are more than one type of service for which solutions are to be explored," according to a copy of the minutes of the meeting obtained by The Associated Press. "Some of them are BlackBerry, Skype, Google etc. It was decided first to undertake the issue of BlackBerry and then the other services."*
>
> *"**They have clearly instructed us that after BlackBerry, they are going to take to task Google, Skype and similar services that bypass the monitoring department of India**," said Rajesh Chharia, president of the Internet Service Providers Association of India, who attended the meeting. "**According to the law, they have to allow monitoring.**"*
>
> *...*
>
> *India is keen to get the U.S. to transfer technologies, like de-encryption, as part of high-level bilateral discussions on technology transfer likely to come up at Obama's state visit to India in November, diplomats say.*[37]
>
> *India eyes Google and Skype in security crackdown (Sep 2010)*

RFC 6. Product Assurance

RFC 6.1

What, if any, changes need to be made with respect to international product assurance institutions, standards, and processes (e.g., the Common Criteria Recognition Arrangement)?

Security certification should be more than just "algorithms" or standards compliance. Independent penetration testing should be an active part of all security testing. Certification should provide some assurance of trustworthiness. See [38] for a discussion by B. Schneier on existing limitations with FIPS 140-2 certification and community security expectations.

RFC 6.2

Should the Common Criteria Recognition Arrangement, the basis for international mutual recognition of cybersecurity product assurance, be expanded to include some of those countries which increasingly stray from international norms?

Yes, expanded inclusiveness sounds good.

---

[37] http://www.usatoday.com/tech/2010-08-13-google-india_N.htm

[38] http://www.schneier.com/blog/archives/2010/01/fips_140-2_leve.html

RFC 8. An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

RFC 8.1

"What are the merits of providing legal safe-harbors to those individuals and commercial entities that meet a specified minimum security level? "

Cyberspace, Innovation and The Internet Economy

See our "Unified Standards Proposal" (found below in this document) for ways in which we feel safe-harbours might be used in the context of supporting the global adoption of national and international cybersecurity standards by organisations of all sizes.

RFC 8.2

"How do national security requirements affect the commercial sector's adoption of cybersecurity protection measures?"

Cyberspace, Innovation and The Internet Economy

As the global community's dependence on the Internet for day-to-day normal communications, the importance of preserving individual privacy increases. However the perverse incentives to intercept and exploit that communications also increases as the number of people dependent on the medium increases. Increasingly organisations that traditionally provided information security to civilians are now also publicly advertising the sale of interception technologies to Governments.

It is clear that national security requirements can have a powerful influence in both encouraging and discouraging (or retarding) security solutions in the civilian space.

Commercial organisations are discouraged from implementing trustworthy security controls if they feel they may face negative Government incentives, particularly if they feel that one or more Governments may block commercial sale of their product. See the recent issues with Blackberry email security in India and Gulf States[39].

It becomes increasingly difficult (if not impossible) for a commercial organisation to implement and achieve trustworthy information security controls on behalf of the civilian client if certain personal use products are mandated to install (covert) legalised interception back doors for Nation states[40]. See China's demand on eBay for interception capabilities on Skype[41]. This trend appears to be increasing. Apparently India may soon ask for interception capabilities on Skype[42]. We observe that the intercepted Skype text in China was transmitted in the clear to be stored on unsecured FTP servers, removing all data-privacy for the user. Security weaknesses in interception systems is not limited to Asia. "*Can they hear me now? A security analysis of law enforcement wiretaps*" [43] which highlights security weaknesses in other "legalised" interception systems. Legalised interception systems may also make security systems weak against foreign attacks[44].

---

[39] http://www.bbc.co.uk/news/technology-10866417

[40] http://www.reuters.com/article/idUSTRE67G3LO20100817

[41] http://blogs.pcmag.com/securitywatch/2008/10/skype_admits_to_helping_china.php

[42] http://www.google.com/hostednews/afp/article/ALeqM5ixoWED9opAi7enDFXTgUdamzsa_A

[43] Sherr, M., Shah, G., Cronin, E., Clark, S., and Blaze, M. Can they hear me now? a security analysis of law enforcement wiretaps. In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security (New York, NY, USA, Nov. 2009), ACM, pp. 512–523. Available at http://www.crypto.com/papers/calea-ccs2009.pdf.

[44] Schneier, B. U.s. enables chinese hacking of google. In CNN Opinion (Jan. 2010), CNN. Available at http://edition.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html.

Commercial organisations may find themselves in complex legal, public opinion, and/or moral situations if they assist the "wrong" government to Intercept communications. See [45] and [46].

In short, it may not be possible to achieve trustworthy security in the civilian sector if Governments, demand to install weak interception technologies.

These factors, taken together, provide strong negative incentives to organisations considering building security in. This means less organisations are offering products that could substantially improve our common security on the Internet. In turn, a lack of trustworthy security promotes an ecosystem of malware and other malicious internet activities that could fundamentally undermine regional and global stability.

On the positive side Government and Industry security compliance requirements in the health care, financial systems and other areas (such as Sarbanes–Oxley, Health Insurance Portability and Accountability Act, Payment Card Industry Data Security Standard, and others) have been a **powerful and visible agent** for promoting the use of strong cryptography and appropriate information security controls and processes within organisations.

We feel that clear and sustained government policies that encourage, support, uphold and defend the legitimate interests of all stake-holders/people in the global community and that employ a system of transparent checks and balances would contribute significantly to creating a trustworthy dependable Internet and global information society.

[45] http://blogs.nokiasiemensnetworks.com/news/2009/06/22/provision-of-lawful-intercept-capability-in-iran/

[46] http://www.guardian.co.uk/technology/blog/2009/jun/22/iran-nokia-siemens-networks

Unified Standards Proposal: developing a unified electronic requirements management process to support international cybersecurity compliance

Please see our paper titled: "*Part 4: The need for the EC to fund the development of an electronic requirements management process to support the conversion of existing standards, existing policy guidelines and existing laws of several nations simultaneously in a unified requirements model that also supports national and regional variations.*"

This paper was previously submitted to NTIA and is available at:
http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Synaptic%203%2Epdf

Our proposal suggests that relevant privacy laws, national and international, such be unified in an electronic requirement model, enabling all organisations to quickly identify what requirements they must satisfy in their software and business processes in their respective jurisdiction. Many other benefits are outlined.

Miles Smid (of Orion Security, formerly Acting Chief of the Computer Security Division of NIST) had this to say about this proposal:

> *"I think that this is an interesting idea and indicates how standards requirements will need to be managed in the future."*