VIOLETA BULC
Member of the European Commission

Brussels, 16. 02. 2016
NvP

[redacted]

Mr Günther OETTINGER
European Commissioner for Digital Economy and Society
BERL 09/024

Dear Commissioner,

Thank you very much for your kind invitation to attend the Europa Forum Lech.

As you know I have a keen interest in the topics on the Agenda. However, I need to attend a combined meeting of Transport and Environment Ministers, scheduled by the Dutch Presidency on 14 and 15 April.

As we already discussed, on 14 April a declaration on connected and automated vehicles will be adopted and I had hoped you could be present as well.

Best regards,

[redacted]
Violeta BULC

Address: European Commission - B-1049 Brussels, Belgium - Tel.: +[redacted] - e-mail: [redacted]

European Commission

[redacted]

Miguel ARIAS CAÑETE
Member of the European Commission

Brussels, 01 FEV 2016
Ares(2016)s 540597

Dear Commissioner Oettinger,

Thank you for inviting me to the Europa Forum Lech 2016 which will be held on 14-15 April 2016.

Unfortunately, I was committed to participate in the Informal Environment Council in Amsterdam on those days and therefore I am unable to attend the Europa Forum.

Nevertheless I will ask my services to be involved and to cooperate with you on the preparations of the respective sessions, as requested in your invitation.

Yours sincerely,

[redacted]

Mr Günther H. Oettinger
Member of the European Commission
Digital Economy and Society

[redacted]

Rue de la Loi, 200
B-1049 Brussels

[redacted]

From: [redacted]@enisa.europa.eu]
Sent: Friday, April 15, 2016 9:54 PM
To: [redacted](CAB-OETTINGER); [redacted](CAB-OETTINGER)
Cc: [redacted](ENISA); [redacted](CAB-OETTINGER); [redacted](CAB-OETTINGER)
Subject: 20160411 Joint ENISA - NXP Statement for Lech: next steps

Hallo,

wir, NXP und ENISA, hatten heute einen Termin mit Kom. Oettinger.

Ziel:
Vertrauen in Produkte (wie HW, SW, Kommunikation) für die Nutzung im Internet zu schaffen. Beispiele: im Reisepass, im elektronischen Personalausweis, in der Gesundheitskarte, im Smart Meter, im Automobilsektor sind Chips von NXP oder Infineon eingebaut, die mittels kryptographischer Kompnonenten sichere Hardware-Anker (HSM=Hardware Secure Module) bilden. Im Reisepass zum Beispiel ein Chip, der das Bild und den Fingerabdruck sicher gegen unbefugten Zugriff speichert.

Hintergrund:
NXP und Infinion sind weltweitführende Halbleiterhersteller. Die einzigen großen Europäischen Player in Europa, und mit Sitz in Deutschland.
NXP hat ENISA vor zwei Wochen in Athen besucht.
Aus diesem Besuch ist das beiliegende Paper entstanden, dass wir heute Herrn Oettinger übergeben haben.

Das Papier, von der Industrie getrieben, enthält Vorschläge, wie z.B.
- Erarbeitung eines 'Baseline IoT Security and Privacy Frameworks'
- Cyber Security Standardisation
- Certification and Labelling schemes
- Procurement Guidelines

Vorgehen:
da NXP und Infineon deutsche Unternehmen sind, wurde ein zweistufigens Vorgehen diskutiert:

1. im Juni eine Gespräch in Berlin,
Ziel: gemeinsames Verständnis der Sachlage und den industriellen wie poliitischen Herausforderungen zwischen Politik, Industrie und Sicherheitsbehörden;
Vorbereitung eines Gespräches in Brüssel.

Teilnehmer: COM Oettinger; [redacted] BSI: [redacted]
ENISA: [redacted]

Zeitraum: Juni

2. im September ein Gespräch in Brüssel
Ziel: da im globalen Wettbewerb nur europäsische Lösungen zielführend sind, gilt es die Ergebniss aus (1) in Einklang mit den Zielen des europäischen Binnenmarktes zu bringen und die Entscheidungsträger in Brüssel zu unterstützen.

Teilnehmer: wie (1) plus DG CNECT Viola, Timmers
da BSI eingebunden ist, ANSSI einbinden

Zeitraum: Sept.

Kom. Oettinger erwähnte, dass er in einigen Wochen [redacted] ANSSI, und [redacted] BSI, trifft; beide sollen vorher über diese Thema gebrieft werden (Aktion: [redacted]

Kind regards,
[redacted]

[redacted]

ENISA's and NXP's Joint Statement on the Security of Smart Infrastructures, Products and Services

1 Scope

This document presents ENISA's and NXP's joint statement on the security of smart infrastructures, products and services in the hyper-connected world. The Internet of Things (IoT) brings opportunities and threats and, above all, will change our world forever.

It identifies key challenges and proposes targeted actions to be taken by public and private stakeholders including the EU Commission.

2 Key Challenges

Radical Transformation in the hyper-connected world

- According to the latest studies, already now two thirds of all Internet users believe their data is not safe online[1]. As the world grows ever more interconnected – in four years 50 billion smart objects will be able to communicate with one another – **threats from data manipulation, data theft, and cyberattacks grow exponentially.** The ubiquitous Internet of Things (IoT) will introduce new threats and risks that need to be studied properly in order to develop appropriate mitigation mechanisms and controls.
- Industry is one of the pillars of the European economy: The manufacturing sector in the European Union accounts for 2 million enterprises, 33 million jobs and 60% of productivity growth[2]. Digital technologies play the central role in value creation in the European economy and bring about radical transformation to all aspects of development, production and related services. **Europe's challenge is to keep its industrial strengths and to fuel this with smart and connected solutions.**
- Trustworthiness of ICT products is necessary for the success of the **European Digital Single Market** as well as the homogeneous implementation of the recent **European legislative initiatives in the area of information security.** Until now, there is no European equal level playing field for security and privacy and there are no rules that international products will have to follow the defined European quality and trust level to stay competitive.

Standardization

- The IoT is used to provide smart and value-added services to citizens (e.g. smart cars) and businesses (e.g. smart factory). As they have a major impact on the safety of their users, the **consideration of security for ensuring safety needs to be centrally addressed** by manufacturers, integrators, and service providers.
- The global standards market in the NIS and cybersecurity domain is **complex and highly specialized** within ICT sectors. It is **increasingly difficult to authoritatively determine if gaps in standardization or in capability exist.**

- The formal recognition processes for technical standardisation have been progressively **side lined in practical form** by the rapid growth, over the past twenty years, of what may be termed **alternative standards development bodies.**

Certification and Labelling

- Despite the numerous discussions taking place during the last years in both public and private sector fora, **there is still no common European framework for security certification** of ICT products.
- As the amount of certified products will rise in the coming years there will be more certification bodies supporting the needs for certification. So far Security Certification is based on the assumption that vendors are honest. However, there are **no measures currently foreseen to allow customers to detect if a vendor is cheating**, i.e. delivering a different product than used in a security evaluation under the same name. This may result in products rolled out being weak or having a backdoor included on purpose.
- Complementary to EU Certification for cyber security products there is a need for the introduction of Trust Labels as a seal of guarantee of security as well as privacy in infrastructure, products and services. Such a label can help corporates and consumers to identify secure providers and determine if the security level of a connected device or service fulfils the personal need for trust. The benefit of this European label resides in its EU-wide recognition and acceptance, thus helping to fight the defragmentation of the European market

Risk Assessment

- Typical developers and service providers of connected devices are not experts on cyber security matters nor give enough attention to this aspect in their products. They reuse third-party development software and have no way of ensuring the security of their devices nor the privacy of their users.
- Often, connected devices are later integrated into a system. The security requirements of this system may not be known to the designers of the devices and vice versa. Hence, risk analysis at the system level requires security and trust labels that help in selecting appropriate components.

3 Key Recommendations

New Regulatory Framework

- **Security and Privacy by Design:** IoT manufacturers and service providers must ensure that their products are secure and will remain so until the end of their life:
  - The **integrity of information** from the connected world – of devices, objects and sensors – needs to be protected at all times. As a base infrastructure, connected devices in the IoT need identities. To protect users' rights in this context, "human" identities must be decoupled from the identities of the devices involved.
  - People and businesses need to retain absolute **control** themselves over who can access data from the devices they're using and what data should be accessible. Connected devices need to be designed in such a way that they protect the user's anonymity or identity.
- **Baseline IoT Security and Privacy Framework:** Thus, a new common framework is needed that establishes **minimum requirements for security and privacy in the highly connected world**, e.g. for **chipsets of connected devices, operating systems, devices, interfaces and communication up to**

the **cloud.** These should be so comprehensive that they apply to all connected objects – whether a connected car or a heating system in a smart home.

- ENISA, in co-operation with all stakeholders, should develop such **Baseline IoT Security and Privacy Framework** based on good practices currently deployed by the stakeholders and in line with the NIS Directive provisions.

Standardization

- With these **Baseline IoT Security and Privacy Framework** related appropriate **cybersecurity standards** should be developed by European Standardisation Organisations (ESOs) with **active involvement of all stakeholders**, including, European institutions, Member States and industry.
- Cybersecurity standards should also allow **full interoperability of products and services.**

Certification and Labelling

- **European Certification Best Practices:** There is already **extensive experience in Europe in the area of certification** thanks to initiatives like the **CE marking** for the go-to-market of products as well as the **Common Criteria** recognition agreements. **Adaptation and extension** towards existing and future infrastructures is needed.
- **System of security certification:** For implementing the standards set down in law, a **system of security certification is required** enabling guaranteed compliance with those minimum requirements and thereby certifying both hardware- and software-based security technology.
- **Extend Security Certification Schemes and Enforcement:** A service must be developed to uniquely **identify if a product given at hand is the certified one.** Short-term this may include user guidance and configuration documentation digitally signed by the certification body together with the certificate. Mid-term the service might include authenticity checks on the product itself, be it physical or logical. In any case, **certification enforcement needs be intensified:** If cheating is detected the related vendor could be blacklisted and all of his certificates revoked.
- **European Trust Label:** A European Trust Label for cybersecurity products, services, and mutual certification, respecting EU values / sovereignty and empowering the national CERT shall be created to help identify trusted European products and services: it could use existing labelling procedures such as the CE Mark, Ecodesign or EU Energy Efficiency Label.

Risk Assessment and Management

- IoT manufacturers and service providers should follow a **Risk Assessment** approach to their product development life cycle. They should also identify and deploy appropriate mitigation measures and controls that would address those risks.

Procurement Guidelines

- **Procurement Guidelines** can assist potential customers of IoT systems and services to better formulate their security requirements. Increased requirements can boost the level of security and privacy integrated in IoT products and services by manufacturers.

Skills

- **Guidelines for skill sets** matching safety and security requirements are required to address the complex cyber-physical risks of smart infrastructures and services. That would help in bridging the skills gap noticed in several organisations offering such smart infrastructures and services.

4 About ENISA and NXP

ENISA assists the European Commission, the Member States and the business community to address, respond and especially to prevent Network and Information Security problems. The Agency is as a body of expertise, set up by the EU[3], to carry out very specific technical, scientific tasks in the field of Information Security. ENISA also assists the European Commission in the technical preparatory work for updating and developing Community legislation in the field of Network and Information Security.

Contact: Dr Evangelos Ouzounis, Head of Secure Infrastructure and Services Unit, ENISA: evangelos.ouzounis@enisa.europa.eu

NXP Semiconductors N.V. (NASDAQ: NXPI) enables secure connections and infrastructure for a smarter world, advancing solutions that make lives easier, better and safer. As a technology developer with decades of expertise for secure connectivity solutions in embedded applications, NXP is driving innovation in the secure connected vehicle, end-to-end security & privacy and smart connected solutions markets. Built on more than 60 years of combined experience and expertise, the company has 45,000 employees in more than 35 countries.

Contact: Eva Schulz-Kamm, Head of Political Affairs & Public Co-Creation: eva.schulz-kamm@nxp.com

[3] ENISA came into being following the adoption of Regulation (EC) No 460/2004 of the European Parliament and of the Council on 10 March 2004. Operations started in Crete in September 2005, after an initial setting up period in Brussels. The new ENISA basic Regulation is the Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, repealing Regulation (EC) No 460/2004.

From: [redacted]@fastweb.it]
Sent: Wednesday, March 02, 2016 1:35 PM
To: [redacted] (CAB-OETTINGER)
Cc: [redacted] (CAB-OETTINGER); [redacted]
Subject: MEETING REQUEST - Europa Forum Lech 2016 (14-15 April 2016) - confirmation letter

Dear [redacted]

Taking the opportunity of the upcoming Lech Forum, we would appreciate the possibility to organise a bilateral meeting between Mr Oettinger and Fastweb's CEO Alberto Calcagno at the margins of the conference. Could you please let me know whether this would be possible?

Many thanks in advance.

Best regards,

[redacted]

—

[redacted]

Fastweb S.p.A.
Rue de Trèves 49
1040 - Bruxelles

Mobile: [redacted]
Direct:+
Twitter:

From: CNECT-EUROPA-FORUM-LECH-2016@ec.europa.eu [mailto:CNECT-EUROPA-FORUM-LECH-2016@ec.europa.eu]
Sent: mercoledì 2 marzo 2016 11:00
To: [redacted]
Cc: [redacted]
Subject: Invitation to the Europa Forum Lech 2016 (14-15 April 2016) - confirmation letter

[redacted]

SecurePIM
by Virtual Solution

An:

Kommissar Günther Öttinger
Europäische Kommission
Rue de la Loi / Wetstraat 200
1049 1049 Brussel
Belgium

München, den 15. März 2016

Sehr geehrter Kommissar Öttinger,

Im Februar 2016 war mein Unternehmen virtual solution AG mit unserer Sicherheits-App SecurePIM Sponsor der Münchner Sicherheitskonferenz.
Wir haben jedem Teilnehmer der MSC unsere Enduser Lösung www.securePIM.com umsonst zur Verfügung gestellt, womit die Teilnehmer in die Lage versetzt wurden, verschlüsselt zu kommunizieren und Datensicherheit auf Ihren Mobiltelefonen zu haben (siehe Beilage).
Gerne würde ich fragen, ob ich beim Europa Forum Lech 2016 auch ein kleiner „Sponsor" bzw. Ausstatter der Teilnehmer mit unserer Sicherheits-App sein dürfte?

Anbei ein kurzes Update unserer Entwicklung:
Wir hatten einen Tag vor der MSC unser Enduser-Produkt der Presse vorgestellt, die einzige sichere Containerlösung, die auf Servern der Massen-Emailprovidern (Google, Yahoo, etc.) läuft, jeden User absichert und E-Mails verschlüsselt, so dass die „Reading-Robots" der Provider nicht mehr die Kundenemails lesen können.

[redacted]

Im Enterprise Markt verkaufen wir über Vertriebspartner [redacted] Lizenzen pro Monat. Das ist für uns ein sehr großer Erfolg.
Wir gewinnen langsam Marktanteil gegenüber den etablierten amerikanischen Lösungen [redacted]

Mit unserer BSI Lösung hat ebnfalls der Pilotbetrieb begonnen. [redacted]

Ich würde mich freuen, wenn wir z.B. den Teilnehmern ein Infoblatt mit QR-Code auf die Zimmer legen könnten, so dass diese dann die Lösung runterladen können und unter einander verschlüsselt kommunizieren können. Falls Sie möchten, dass ich zum Thema Cyber Security rede, stehe ich Ihnen selbstverständlich zur Verfügung.

Unabhängig davon freue ich mich auf das Europa Forum Lech und bedanke mich ganz herzlich, dass ich wieder teilnehmen darf.

Mit freundlichen Grüßen

[redacted]