Assessing the Impacts of Aligning the Conformity Assessment and Certification in EU Aviation Security

After the 9/11 attacks various governments concluded that investments in innovation and additional research and development are needed in various domains of aviation security. The main focus of the investment was put on the development of new technologies. This paper aims to provide the outcomes of an impact assessment of the conformity assessment and certification (CAC) of security in the European aviation. The impact assessment conducted was part of a study led by Ecorys on behalf of EC DG Enterprise and Industry. At first, the background of the study is explained and importance of reliability of the overall aviation security system is underlined. Need for economically sound decisions is addressed. Next, specific aspects of the aviation security system are discussed. A distinction is made between continuous and disruptive security. The methodology used for the impact assessment is described and the aviation related results are presented. Finally, conclusions are drawn on the need for aligning the regulations and common recognition of conformity assessment and certification in aviation security in view of the outcomes of the impact assessment conducted.

by: Jolanta Rekiel and Robert Piers

Introduction on the 9/11 Aftermath and Security Market Fragmentation

After the 9/11 attacks various governments concluded that investments in innovation and additional research and development are needed in various domains of aviation security. The main focus of the investment was put on the development of new technologies.

A thorough analysis of the European security industry was done by Ecorys on behalf of the DG ENTR in 2009 (Ecorys, 2009). The study showed that the security market in the European Union is highly fragmented. The market development and implementation of various security measures differ per sector as well as per Member State. This was identified as a significant factor negatively affecting the development of the security industry within the EU. According to the outcomes of the study, the security market fragmentation: (1) may lead to higher costs for European industry as well as procurers and users of security products, (2) is unattractive for the future development and long term competitiveness of the security industry, (3) it raises considerations for future growth and employment prospects in a sector associated with a high potential for

technology development and innovation, (4) it may weaken Europe's position in terms of access to and control over technological developments in the security field.

Following discussions by the ESRIF[1], a European Commission Communication underlined the need for a harmonised regulatory framework in specific areas combined with upstream coordination given the fragmentation of the security market, often due to diverging national legislation (EC, 2009). The same Communication said: "Based on the requirements of the end-users and the results of research, new technologies and solutions need not only to be validated; they should also be certified and where appropriate standardised, so they can become part of an effective response to security threats. […] Meanwhile, the Commission is exploring ways in which the results of relevant research actions could be tested in view of developing future certification / conformity assessment procedures mechanisms. Such mechanisms should aim at certifying that security products and processes are in conformity with relevant standards."

Study Objectives

Following the discussion on market fragmentation and the need for aligning of conformity assessment and certification in the security domain in Europe, a study was launched in 2010 by the European Commission Directorate General for Enterprise and Industry (DG ENTR). The objectives of the study were to provide a snapshot of the regulatory framework applying at national and EU level to the security sector, to analyse where national legislation is diverging in such a way that EU level harmonisation may be warranted, to provide a detailed overview of the rules and regulations applying to certification / conformity assessment procedures at national and EU level, and to provide a policy and cost-benefit analysis of various options.

The analysis was done in order to identify possible options for speeding up certification / conformity assessment procedures. The options studied in detail were focused on keeping currently existing systems, but establishing (1) a light coordination mechanism at EU level, (2) an EU-wide certification / conformity assessment procedures system covering all security products and (3) an EU wide fast-track system for the approval of priority technologies. The last part of the study was intended to provide an analysis of the impacts of each of the policy options in order to provide a sound basis for decision makers.

Need for Impact Assessment

The European Union and its Member States should ensure the existence of the conditions necessary for the competitiveness of the Union's industry which reflects the provisions written in the TFEU[2]. The Member States should act in accordance with the system of open and competitive markets by increasing the speed of industry adjustments, encouraging initiatives favourable to industry development (small and medium-sized enterprises in particular), encourage cooperation between them, lead to better exploitation of the industrial potential of policies of innovation, research and technological development. In order to implement various policy initiatives aimed at these goals, the policy initiatives should be assessed from the point of view of their potential economic, social and environmental consequences. An impact assessment is a set of logical steps that prepares evidence for political decision-makers on the advantages and disadvantages of possible policy options by assessing their potential impact[3].

Impact assessments are based on an integrated approach that take into account both benefits and costs of initiatives. They address all significant economic, social and environmental impacts of possible new initiatives. The impact assessment process structures and supports policy development and identifies: (1) the problem at stake and the objectives pursued, (2) the main options for achieving the objective and likely impacts on the economy, environment and society, (3) advantages and disadvantages of each option and examines possible synergies and trade-offs.

The impact assessment may also provide explanation why no action is needed on the EU level.

To conclude, an impact assessment is needed to ensure economically sound decisions by decision makers. The policy options developed within the study conducted should, therefore, be assessed from the point of view of their economic, social and environmental impacts.

Aviation Security System

Specific Aspects of Security in Aviation

Aviation is the most regulated mode of

transport both from the point of view of passenger as well as cargo security measures. The aviation security system is usually broken down into three building blocks, these are technology, process and people (IATA, 2012). Over the last years the main focus was put on the technology development, while its level of development and deployment substantially differs per Member State. There is, therefore, a strong need to ensure a balanced combination of measures that would include all three elements as well as make sure that the technology being developed is capable of addressing the actual security risks.

Despite strict security measures in aviation, security incidents happen occasionally. This affects the air traffic, revenues and costs of aviation stakeholders, feelings of (in)security of passengers. Incidents also affect the decision makers who may implement security measures. The regulation is often adapted as a response to the occurring events. The regulation following an incident is often implemented for months or years. According to Bailey (2002), the new role of governments is not designed to intervene in airline economic decisions but it rather contributes to long-term structural change in the aviation security. A good example is the UK/US airline bombing plot in August 2006. The terrorist tried to get liquids on the plane with the intention to construct an improvised explosive device (IED). The attempt was stopped while the passenger never boarded the plane. Only a few days later the passengers both in Europe and USA (and subsequently in many countries worldwide) were prohibited from taking any liquids, gels and aerosols in their cabin luggage. Shortly afterwards, this was changed and a regulation enabling the passengers to carry liquids, gels and aerosols in containers of maximum 100ml and in total not exceeding 1000ml stored in a plastic bag was imposed. The impact assessment of this regulation was not done prior or after its implementation. Airports were not prepared for its execution without affecting their operations. After the regulation entered into force, August 2006 was a month where extended duration of security checks was a major cause of delays in Europe. Initially, the temporary ban on liquids, was envisaged to be addressed by the new technological inventions that would enable for the chemical composition checks of the liquids carried by passengers. This, however, takes time. After a technology is developed, it has to be tested against strict criteria (that have to be developed). It has to pass the conformity assessment against the existing regulations. It should also, when possible, be certified by dedicated bodies (this means that standards for such a certification should also be developed). Finally, the equipment needs to get the passenger acceptance. Approximately six years after the incident, the temporary regulation is still in place while there is no comprehensive solution implemented in the whole EU.

Table 1: *Main characteristics of market-product segments*

	Type-1 (General security products)	Type-2 (High security products)
Threat type	'Continuous' / 'Endogenous' (e.g. ordinary criminal activity). Threats are generally known and their evolution is relatively predictable.	'Disruptive' / 'Exogenous' (e.g. terrorism, organised/ international crime). Threats are often unknown and their evolution is unpredictable.
Products / technology	'Established/mature'. Technology development based on incremental improvements.	'New/immature'. Technology development is in reaction to new threats or market opportunities.
Operational approach (security function)	Handled in traditional way: technology used to assist human security functions.	Trend towards automation of security functions: human activity substituted by machines/systems (e.g. eGates instead of manual border control; body scanner instead of manual body checks).
Demand	Largely market driven.	Largely regulatory driven.
Standards and CAC standards	Existing national standards and conformity assessment and certification (CAC) (legacy systems) with limited EU-level harmonisation.	No or limited standards and CAC (either at national and EU-level).

Short time is needed to develop security measures and respective regulations to ensure adequate response to a particular threat. Long time is needed, however, to develop advanced technologies that would address the threat as well as have no or limited impact on the operations. It is important to make sure that the measures implemented address the existing security threats in an appropriate way. The technology being developed should be innovative and competitive but also addressing the actual needs. It is crucial that the equipment, procedures and people are reliable and it is possible to check their effectiveness.

Continuous and Disruptive Security in Aviation

Equipment used for maintaining or increasing aviation security levels is part of physical security measures. The equipment used includes technologies used for both 'continuous' security and 'disruptive' security (Ecorys, 2009). The main characteristics of these two types of threats and products are presented in Table 1.

In principle, 'continuous' security can be referred to general security products that are mainly aimed to address traditional security threats (e.g. 'ordinary' criminal behaviour). They may also form part of measures to address 'high-level' or priority security threats. These refer to General purpose security products and solutions (Type-1) aimed at addressing 'familiar' security situations (security threats or functions) through the application of improved but existing technology. The examples of such products include e.g. intruder alarms, access control, CCTV surveillance, etc.).

'Disruptive' security refers to counter terrorism measures or in response to other identified EU priority security threats. The products and solutions covered in this category can be referred to as Priority and sensitive security products and solutions (Type-2). They address 'unfamiliar' or new types of threats that require the development or application of new technologies, and equipment and may be extended to changes in or-

ganisation and implementation of security functions, for example through the automation of security functions. The types of products covered by this category would include newly developed technologies (i.e. corresponding to products/technologies developed primarily to address threats as terrorism, organised crime, cyber-crime, etc.).

Areas of Concern in Conformity Assessment and Certification (CAC) in Aviation Security

Following the definition of the European Committee of Standardization, "conformity assessment is a demonstration that specified requirements relating to a product, process, system, person or body are fulfilled[4]. The purpose of conformity assessment is to provide confidence that applicable requirements have been met. Such confidence contributes to the market acceptance of these products, services and systems. The generic term conformity assessment includes activities such as testing, inspection, certification and accreditation."

The security system at airports focuses on three main elements: processes, people and technology. The technology deployment differs per country and per airport. There are various reasons for this including different needs of the airports due to the size or type of connections, security levels in specific country, airport competitiveness, etc. Some airports can be the weaker point in the overall European security system from the point of view of technology deployment but they can compensate with more focus on the procedures or people. A more streamlined technology deployment should be ensured, but what is more important is the need for a common approach to certification and conformity assessment of security equipment against common standards in Europe. At present, producers of security equipment often have to validate the same equipment against different standards in different countries which delays the deployment. In some cases, the airports cannot fully check the performance of the equipment. The results of the study conducted show two main areas of concern with regard to existing CAC frameworks. The first area would be the absence of common certification systems for security products at a European level and no mechanism of mutual recognition across countries of products certified at a national level – applicable to Type-1 products. There is need for a common EU-wide certification of Type-1 products. The second area of concern would be slow speed of response and adaptation of certification procedures notably where new security threats require the implementation of new security solutions and technologies – applicable to Type-2 products. There is a need to ensure minimum security performance levels (and promoting higher ones) and speeding-up the deployment of new technologies and solutions (Type-2).

These concerns lead to the potential for EU-wide policy initiatives to improve conformity assessment, testing and certification of security products, by enhancing approvals and certification procedures and infrastructure throughout Europe. In principle, the initiatives could either be designed to generate new certification strategies or to harmonise existing ones. Additionally, increased transparency of procedures and improved level and quality of interaction between approval and certification bodies could raise the efficiency of the system and support EU security technology development.

Ex-ante Impact Assessment

Outline of Policy Options

To identify and assess the potential impacts of possible EU-level initiatives to enhance conformity assessment and certification of security products, three policy options have been defined within the study conducted.

Option 1 is the baseline option. The baseline scenario represents a continuation of the currently existing situation. Here, no common EU-wide system providing conformity assessment and certification (CAC) of security products would exist. Security products subject to approval/certification requirements would continue to undergo national testing, validation and approval/certification procedures. No priority would be given to certain products. Furthermore, no additional development of EU-level structures and processes for the implementation of conformity assessment and certification requirements and procedures would take place;

Option 2 is a "A step by step approach". The second scenario would apply to the two market-product segments described above (i.e. Type-1 and Type-2) and would consist of two sub-components. The first sub-component would be Option 2.1 - EU CAC for 'general purpose' security products (Type-1).It would be intended to cover security products aimed at 'general' security markets and/or based on comparatively mature

technologies (Type-1). The second subcomponent would be Option 2.2 - EU CAC for 'priority and sensitive' security products (Type-2). It would be intended to cover security products aimed either at 'specific' markets and/or based on comparatively new or innovative technologies (Type-2). For each product type it is assumed that a step-by-step approach would be adopted under which EU initiatives start with limited product category coverage, to be expanded over time and in response to changes in security-based and market-based priorities. Criteria for the prioritisation of product categories should include (non-exhaustive): (1) EU Internal Security Policy: to ensure the rapid and effective deployment of security products/technologies to address the most pressing security threats and challenges, (2) EU Internal Market Policy: considerations would relate to the prevalence and magnitude of barriers to trade and to the extent to which there is a lack of a 'level playing field' within the EU. EU Industrial Policy with the potential to reduce costs and administrative burden placed on manufacturers/suppliers of security products as a result of existing CAC requirements as well as with the potential contribution that an EU-wide scheme could make to enhance the competitiveness of the EU security industry, (3) Remaining considerations should include speed and ease of implementation and long term benefits for industry, customers and citizens.

Finally, option 3 would be "An all-encompassing approach". This would be a situation where an EU-wide CAC system is in place for all security products (both Type-1 and Type-2) all at once.

Impact Assessment Results

The sensitive nature of security sector has impacted the possibilities for quantification of potential impacts of the policy changes as well as in specific cases even their qualification. Both the supply and demand side of this sector are reluctant to provide measurable data or information that would enable the quantification of the impacts. The reasons for this are mainly the sensitive nature of the security sector as well as commercial aspects. Additionally, little is known on the actual size and scope of CAC activities by different authorities. The impacts, therefore, have not been quantified but are treated qualitatively.

The main identified impacts described below can be associated with the Option 2 when compared to the Baseline Scenario (as described above). The impacts for Option 3 are expected to be of similar nature, they are expected to be larger in magnitude than the impacts of Option 2. Option 3 is, however, treated as significantly less feasible from a technical and political perspective than Option 2. The main impacts have been divided into impacts on different stakeholder groups.

Impacts on producers

Main impacts for producers from an EU certification scheme (with mutual recognition) are reduction of costs associated to multiple testing to obtain national certification, reduction of adaptation costs to meet national product standards/specifications, reduction of the need for product trials (for Type-2 products), reduction of the 'time to market' of products, improved alignment of production to the expected EU market as a whole, reduction of risk that competitors are able to 'replicate' new product developments and innovations, enhanced transparency of performance requirements and standards / specifications (Type-2 products), acceleration of development process (Type-2 products).

Potentially negative impact for producers relates to the additional costs of obtaining EU certification (for products that are currently not covered by national conformity assessment and certification requirements but that will be brought within a future EU-wide system).

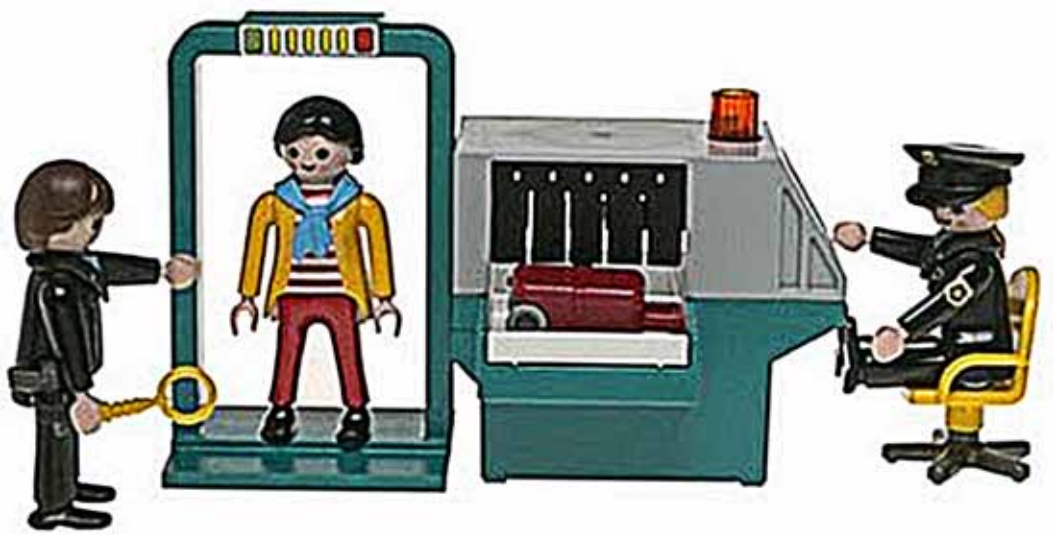
Impacts on market conditions

Potentially positive impacts on market conditions are increased transparency regarding product performance, increased market openness, increased competition in security product markets, increased competitiveness of European manufacturing industry.

The main identified potentially negative impact on market conditions concerns the possibility that minimum EU standards may become de facto market requirements. This may, in turn, reduce the market opportunities for products with performance levels above minimum requirements and, reduce, incentives for investments in RTD to raise product performance. Similarly, it may limit market acceptance of 'alternative' or innovative' products, particularly if they are more costly than standard products that comply with minimum requirements.

Impacts on procurers and users

The main identified potentially positive impacts for procurers and users are lower price for security products, increased product choice / availability, enhanced information / transparency on product performance, facilitation of procurement procedures, reduced uncertainty of compliance with (user) security regulations.



Impacts on conformity assessment and certification bodies and systems

The potential impacts identified for conformity assessment and certification bodies are change in the volume of demand for CAC services, increased competition for the provision of CAC services, strengthened EU-wide accreditation, increase of administrative costs related to the CAC system.

Impacts on regulators

The main impacts identified for regulators are conformity with EU standards as a basis for national regulations and facilitation of regulations through existence of conformity assessment infrastructure.

Impacts on society

It is conceptually difficult to measure the impact that the introduction of an EU-wide conformity assessment and certification scheme would have on society as a whole and on the security of individuals, businesses etc. In this context the expected impacts on society are raised average security performance characteristics of deployed products and accelerate the deployment of security products.

Notwithstanding the expectation that an EU-wide CAC system would raise the performance characteristics of security products, the development of an EU-wide CAC system does not remove the fact that security will only be enhanced if the overall systems (including procedures and processes) are appropriate. Thus, the need remains to evaluate broader security systems (e.g. 'concepts of operation'); including whether the products employed within the system are properly integrated and appropriate given the threat/risk assessment.

Conclusions

The identification and assessment of the potential impacts of possible EU-level initiatives to enhance conformity assessment and certification of security products (also in aviation) led to development of three policy options. The impacts of the policy options were assessed qualitatively due to the sensitive nature of the security sector. The most important impacts expected from the EU wide Conformity Assessment and Certification in the aviation sector are (1) reduction of costs associated to multiple testing to obtain national certification and the adaptation costs to meet national product standards/specifications of x-rays and scanners used at airports and therefore reduction of the aviation security products prices, (2) reduction of the need for new product trials such as security scanners or biometrics, (3) reduction of the 'time to market' and development process of security products in aviation, (4) enhanced transparency of performance requirements and standards / specifications of aviation security products and raised average security performance characteristics of security products in aviation, (5) increased transparency regarding aviation product performance and facilitation of procurement procedures for the airports, (6) increased product choice / availability, competition and competitiveness in aviation security product markets, (7) strengthened EU-wide accreditation but increase of administrative costs related to the CAC system, (8) conformity with EU standards as a basis for national regulations in aviation, (9) facilitation of regulations through existence of conformity assessment infrastructure and acceleration of the deployment of security products in aviation.

To conclude, a more streamlined technology deployment and a common approach to certification and conformity assessment of security equipment against common standards in Europe are very important in ensuring high security levels at European airports. A step by step approach for EU CAC for 'general purpose' security products and an EU CAC for 'priority and sensitive' security products is expected to have numerous positive impacts for the equipment producers, market conditions, procurers and users, conformity assessment and certification bodies and systems. They are also expected to bring some positive impacts on regulators and society, these impacts are more conceptually difficult to measure.

Note from the Authors

The authors wish to point out this disclaimer: In accordance with Article II.10.3 of the Framework Contract ENTR/2009/050, any opinions expressed in that SECERCA study are those of the Contractor (i.e. ECORYS) only and do not represent the Commission's official position.

End Notes

1 European Security Research and Innovation Forum
2 The Treaty on the Functioning of the European Union, Article 173(1)
3 http://ec.europa.eu/governance/impact/index_en.htm
4 Definition according to EN ISO/IEC 17000

About the Authors

Jolanta Rekiel works at Ecorys Nederland BV where she is the Security Studies Manager. She is also a PhD candidate at the University of Amsterdam, at the Faculty of Economics & Business in The Netherlands. Jolanta is a member of the Editorial staff of AerlinesMagazine. Jolanta is a corresponding author for this article. You may contact her at: J.M.Rekiel@uva.nl, jolanta.rekiel@ecorys.com

Robert Piers is a Senior Consultnat at Ecorys Nederland BV, AG Freight, Ports, Air & Space, Rotterdam, The Netherlands. Robert can be reached at: robert.piers@ecorys.com"

References

Bailey, E. E. (2002). Aviation Policy: Past and Present. Southern Economic Journal, Vol. 69, No. 1.
Carafano , J.J. (2008). Fighting terrorism, addressing liability: a global proposal, Backgrounder, published by the Heritage Foundation. May 21, 2008. p. 1-2.
CEN, http://www.cen.eu/cen/Services/ConformityAssessment/Pages/default.aspx
EC. (2009). A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations. COM(2009)691 final.
Ecorys. (2009). Study on the competitiveness of the EU security industry.
Ecorys (2011), Security Regulation, Conformity Assessment & Certification, Final Report – Volume I: Main Report, European Commission, DG Enterprise & Industry, Brussels

Photo credits

Page 1: Terminal overview at Amsterdam Aiport Schiphol. Photo by Du Saar Photography
Page 2: "Have you declared it?" at Antwerp Aiport. Photo by Du Saar Photography
Page 4: Ground security at Amsterdam Airport Schiphol. Photo by Du Saar Photography
Page 5: Airport Security play set by Palymobil. Photo by courtesy of Playmobil.