PSC-Europe/024-2013

Mandate M/487 to Establish Security Standards
Final Report Phase 2
Proposed standardization work programmes and road maps

PREPARED BY:	European Commission
DATE:	10-10-2013
PSC Europe:	Information

REF: PSC Europe/024-2013

PSC Europe: DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	European Commission	PSCE Secretariat	05-07-2013
ISSUED BY	PSCE Secretariat	PSCE Secretariat	10-10-2013

PURPOSE	
Information	X
Reply requested	

In assignment of:

European Commission
DG Enterprise and Industry
Security Research and Development

Mandate M/487 to Establish Security Standards

Final Report Phase 2

Proposed standardization work programmes and road maps

NEN Industry

P.O. Box 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft
The Netherlands

T +31 15 2690135
F +31 15 2690207

security@nen.nl
www.nen.nl

Netherlands Standardization Institute

M/487 has been accepted by the European Standards Organizations (ESOs).

The work has been allocated to CEN/TC 391 'Societal and Citizen Security' whose secretariat is provided by the Netherlands Standardization Institute (NEN).

Mandate M/487 to Establish Security Standards

Final Report Phase 2

Proposed standardization work programmes and road maps

REPORT VERSION	**REPORT DATE**
Final report	05-07-2013

Although the utmost care has been taken with this publication, errors and omissions cannot be entirely excluded. The European Committee for Standardization (CEN) and/or the members of the committees therefore accept no liability, not even for direct or indirect damage, occurring due to or in relation with the application of publications issued by the European Committee for Standardization (CEN).

.

Contents

Page

Executive summary

Mandate M/487 was performed in order to analyse the existing security standardization landscape, select priority sectors and develop standardization roadmaps for three selected security sectors to support EU policy on security.

- Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE);
- Border Security – automated border control systems (ABC), as well as biometric identifiers;
- Crisis Management/Civil Protection –communication interoperability and interoperability of command and control, including organizational interoperability, as well as mass notification of the population.

The work on Mandate M/487 was led by CEN TC 391 Societal and Citizen Security, secretariat NEN (Dutch National Standardization Body). For each of the three sectors an internationally recognized expert was assigned to support the work.

For each of the sectors a two day workshop was organised at which standardization proposals were discussed that had been collected prior to the workshops. Stakeholders were asked to give their proposals in a template indicating the impact, urgency, end users etcetera. More than 300 proposals were discussed and prioritized by more than 200 participants. Feedback and comments were given by an even much larger number of stakeholders. There was a balanced participation of stakeholders in this process, coming from security industry (including SME's), research institutes, end users, consultants, standard experts and local, national and international authorities. The workshops were evaluated and the feedback showed that the participants appreciated the way this process was organized.

Border security. Every day millions of people cross European external borders. European border control can be more efficiently managed and secure with the help of standards.
Automated Border Control (ABC) is likely to become a permanent feature at many passport controls in Europe and worldwide by the end of this decade. The priorities for standardisation lie in three main fields:

- Commonality of technical standards for the components so that operators know exactly what they are purchasing and how it will perform;
- Commonality of the 'look and feel' of ABC systems so that passengers intuitively know how to use different systems;
- Commonality of standards for the operators' interface so that border agency staff are protected from stress and physical strain.

Crisis management and civil protection. The floods in June 2013 in central Europe as well as major recent storms, sanitary crises, severe accidents or terrorist threats or attacks show the need for crisis management and civil protection standardization activities to facilitate response, effectiveness, efficiency and cooperation.
Standardization for interoperability in crisis management should:

- first consider semantic, planning, resilience and organizational interoperability issues, as prerequisite for additional work;
- then some pragmatic technical and syntax aspects, with a bottom-up approach (looking at first responders needs and mass notification to the population), as conditions for rapid operational improvements;
- lastly, and in the longer term, communication interoperability between command and control centres, as enablers of coordination and cooperation efficiency".

CBRNE. There are evermore people at risk from CBRNE accidents like the derailed train carrying hazardous chemicals at Wetteren, Belgium, with release of poisonous gases. Or a terrorist attack, using homemade explosives based on fertilizer, on a part of the critical infrastructure. Standards for sampling and detection and protective equipment for first responders will help improve protection of first responders, citizens and workers.
Furthermore:

- There is broad consensus under the participants in this project that for most efforts aimed at an increase in 'impact' and/or 'defragmentation' in the field of CBRNE to be effective, some degree of international 'standardization' will be required – both as a way to *regulate* ('top-down') as well as a way to *learn from others and to overcome resistance/roadblocks* ('bottom-up').
- There is insufficient (meta) information currently available to link and provide an overview of various projects, programs, products, technology, market segments and 'lessons learned'/residual knowledge on best practices - within and between the various stakeholder categories.
- Aside from the specific priority actions ('quick wins') identified, a common and shared frame of reference needs to be developed which includes action to be taken on items as diverse as '*semantics and terminology*', '*system modelling*' and '*cost-benefit analyses of (joint) resource and asset protection*'

Although there are many current research and standardization-like projects in these three areas, it appears that a significant number of stakeholders were not well informed about standardization, its deliverables and processes.
This is something that the European Standardization Organizations should resolve. **Once introduced to standardization and the advantages of standardization stakeholders considered standardization an important market tool**.

The proposals with the highest impact and urgency in each of the three sectors are given in three tables in chapter 3, based on the expert judgement of the stakeholders on market need, impact, realization of the EC objectives and so on. Also clusters of proposals are given as roadmaps. No exact costs of future work on the proposals can be given in this report. Costs depend on the type of deliverable, the way work is going to be organized and so on. The European Commission and the ESO's will have to negotiate on this.

Apart from the concrete standardization roadmaps for the three sectors and lists of recommendations, the report states the positions of different stakeholder communities concerning potential standardization work as well as some general aspects that are of relevance for the sector such as confidentiality, integrity, safety versus security.

Note: See Annex A for a key to all abbreviations used.

Contributions

A large number of stakeholders from all over Europe have contributed to this report by sending in proposals, participating in the workshops, being interviewed by the experts, or commenting on the draft report.
Their expertise, knowledge, time and effort helped very much to fulfil the work of this phase of the Mandate.

1 Introduction and objective

1.1 Context

Providing security is a central concern of any society. A safe and secure environment is the very basis on which any stable society is founded. A competitive security industry offering solutions for enhanced security can make a substantial contribution to the resilience of European society.

The European Commission's Action Plan for an innovative and competitive security industry [1] shows that the security market in Europe is a highly fragmented, institutional market with a strong societal dimension. Highly fragmented because of e.g. the lack of standardization and harmonised certification and with a strong societal dimension because it is most likely that whatever is developed touches citizens in some way.

One of the aims of the European Commission with regard to the security market is to establish a better functioning Internal European Market for these security technologies. The execution of Mandate M/487 [2] is a first step towards this goal.

Many of these problems can (at least partially) be overcome by creating EU wide or international standards, harmonization of EU certification/conformity assessment procedures for security technologies and exploitation of synergies between security and defense technologies.

Standards play a major role in defragmenting markets and helping industry in achieving economies of scale. Standards are also of upmost importance for the demand side, notably with regard to interoperability of technologies used by first responders, law enforcement authorities, etc. Additionally, standards are essential for ensuring uniform quality in the provision of security services. Creating EU-wide standards and promoting them on a worldwide level is also a vital component of the global competitiveness of the EU security industry.

However, few EU-wide standards exist in the security area. Divergent national standards seem to pose a major obstacle for the creation of a true internal market for security, thus hindering the competitiveness of EU industry.
The Commission has already announced in its Communication on a Strategic Vision for European Standards [3] the need to speed up standardization efforts in the security area. Therefore, with the issuing of M/487 the Commission mandated in 2011 the European Standardization Organizations (CEN, CENELEC and ETSI) [1] to gather a detailed overview of existing international, European and national standards in the security area, as well as to set out a list of standardization gaps and to propose a standardization work program.

The Mandate has been accepted by the European Standards Organizations. The work has been allocated to CEN/TC 391 ‘Societal and Citizen Security’ whose secretariat is provided by the Netherlands Standardization Institute (NEN).

[1] CEN, European Committee for Standardization
CENELEC, European Committee for Electrotechnical Standardization
(CEN and CENELEC are one organization)
ETSI, European Telecommunications Standards Institute (ETSI is a separate organization)

The work on the mandate consists of two phases:

- *Phase 1* — to provide the result of a preparatory study and a list of sectors for priority treatment (Report published May 2012) [1];
- *Phase 2* — based on EC reaction to the output of Phase 1, to propose standardization work programmes and roadmaps related to the selected sectors.

Phase 1 focused on obtaining an overview of the current security landscape and a listing of the sectors for priority treatment to be agreed upon by the Commission. In the Phase 1 report it was recommended that a start could be made with the following six priority-sectors:

- Border security
- Aviation security
- CBRNE
- Crisis management/civil protection
- Personal data protection
- General coordination of European security standardisation

Phase 2 required an in-depth study within three selected priority sectors (see1.3), identifying the gaps in standardization and on developing respective roadmaps for work to fill the most urgent gaps.

This report gives the overall results and the methods used in Phase 2 to produce them.

1.2 Objectives

In order to promote EU industry in these sectors and to promote the security of the citizen, identification of the specific standardization needs and preparation of a comprehensive standardization programme with suitable and realistic roadmaps, has been undertaken. The roadmaps for the selected sectors are included in chapter 3.

Based on Phase 1, the European Commission has formulated the following overall objectives for Phase 2:

- To increase the harmonisation in the European security market and reduce fragmentation by the creation of a set of comprehensive European standards.
- To enhance secure interoperable communications and data management between the various security control centres, operators, public authorities and first responders.
- To develop common technical specifications concerning interoperability, quality or safety levels, including test methods and certification requirements.
- To provide interoperability and comparability of different solutions, which in turn facilitate competition and innovation.
- To develop methods for security vulnerability assessment by security system operators.
- To allow companies the opportunity to develop tailor-made and cost beneficial security measures in agreement with a global EU security strategy.

1.3 Scope

Mandate M/487 concerns the development of a programme for European standards (and other standardization deliverables) for security[2], taking note of specific products, systems, procedures and protocols to assist the EU to get interoperability frameworks including e.g. minimum performance standards in different security landscapes. It has an exclusively civil application focus.

Therefore, the mandate required an analysis of the current security standards landscape, including legislative background, in order to draw roadmaps for the development of the missing or defective standards.

The analysis covers existing formal European and international standards documents, and the ESOs have drawn up roadmaps to provide any missing standards or amend existing standards to meet current requirements on the selected priority sectors.

According to the outcome of Phase 1 of this project, in Phase 2 there were 3 selected security sectors addressed;

- Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) – minimum detection standards as well as sampling standards, including in the area of aviation security;
- Border security – common technical and interoperability standards for automated border control systems, as well as standards for biometric identifiers;
- Crisis management/civil protection – standards for communication interoperability, as well as interoperability of command and control, including organizational interoperability, as well as mass notification of the population.

Human factor issues, privacy concerns and identification of operator requirements for enhancing systems effectiveness can be expected to be relevant to all the topic areas listed. With the exception of Cryptography, as it is considered a key technology for any security application, the Information and Communications Technologies (ICT) are not covered by mandate M/487. However, specificities which rise from their adaption to the field of security are included in it.

1.4 How to read the document

After the introduction in chapter 1, chapter 2 describes the method that was used in this phase 2 of Mandate M/487, including a description of 'standardization'. Chapter 3 gives general recommendations (chapter 3.1) and an overview of the results on Border security (chapter 3.2), Crisis management (chapter 3.3) and CBRNE (chapter 3.4). Follow-up on this report is discussed in chapter 4. For the many abbreviations that are used in this report the reader is referred to Annex A.

In Mandate M/487 there are some specific questions included. These questions are worked out in the text of this report.

[2] The security concept here includes protection against natural or man-made disasters like the effects produced by earthquakes, volcanoes or pandemics. It excludes defence and space technology, the latter for which a programming mandate has already been issued by the Commission (Mandate M/415 'Programming Mandate addressed to CEN, CENELEC and ETSI to establish Space Industry Standards')

2 Process

2.1 Methodology

The work for the Mandate was led by CEN TC 391, Societal and Citizen security and has been the same during the whole project with one exception. In phase 2 for each of the selected security sectors an expert has been assigned to work out the roadmaps. These experts (Chris Hurrey (Border Security), Alain Coursaget (Crisis Management and civil protection) and Eelco Dykstra (CBRNE) were also members of the Coordination Group.

The organization was as follows:

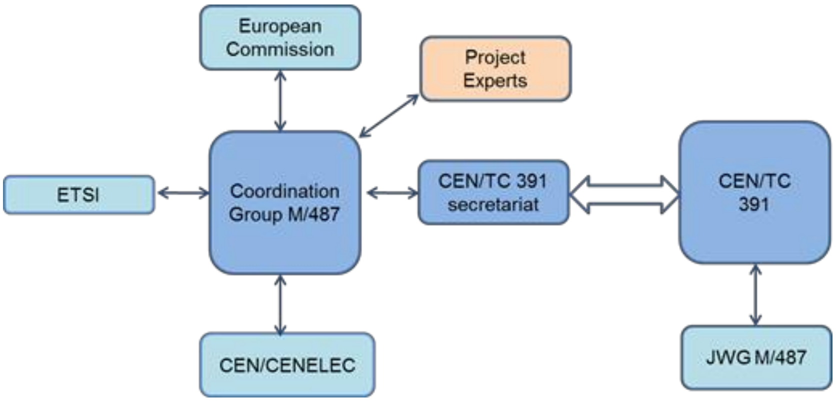


Figure 1 — Coordination of the mandate work

All stakeholders identified in phase 1 were invited to participate in the work of phase 2. For phase 2, for each of the three sectors, the work was carried out in three stages:

- Existing standards and recommended practices and identification of standardization needs.
- Development of standardization programmes with roadmaps.
- Communication of the results.

Three workshops were organised in April 2013, each focusing on one of the three sectors. In preparation of the workshops, the experts gathered information by carrying out a document study and interviewing several key stakeholders. The outcomes of those interviews are included in the results and roadmaps and therefore are part of this report. Also a template was developed for standardization proposals where stakeholders were invited to indicate the impact, market needs, end users and so on.

All stakeholders have been invited to submit standardization proposals not later than two weeks prior to the workshops. The experts grouped the proposals in work streams to organize the discussions at the workshops. During the workshops all of these proposals were considered and the following questions were asked:

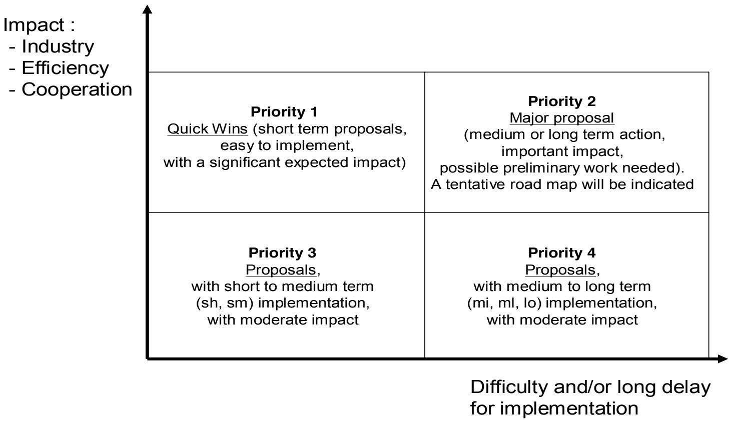
- Do we recognize the proposal as valid and relevant?
- Is it a subject for standardization in the scope of the Mandate and the scope of the workshop?
- What will be the impact and advantage of standardization?

- At what term (long, medium, short) can a standard or other deliverable be developed?

After the workshop every participant received an overview of the outcome and had the possibility to comment react on it. Details of each workshop are in Chapter3.

2.2 Selection criteria

The document study, the interviews and the submitted proposals for standardization for the workshops provided a good deal of relevant information. During the workshops all proposals were judged on impact and time required for implementation. Based on these parameters, the proposals were prioritized as shown in figure 2.



Priority 1
Quick Wins (short term proposals, easy to implement, with a significant expected impact)

Priority 2
Major proposal
(medium or long term action, important impact, possible preliminary work needed).
A tentative road map will be indicated

Priority 3
Proposals, with short to medium term (sh, sm) implementation, with moderate impact

Priority 4
Proposals, with medium to long term (mi, ml, lo) implementation, with moderate impact

Figure 2 - Priority criteria

Every proposal was discussed in terms of benefit for industry and better security and the possibility to be developed on short term. Priority 1 was given on issues with a significant impact/benefit for industry and with an indication that it could be developed on a short term. Priority 4 on the other hand has less/moderate impact and needs more time to develop/implement.
All stakeholders were invited to comment on the outcomes of each workshop before May 5 and to comment on the draft report in a six week commenting period starting May 13.

Also for synergy and to avoid double work, standardization proposals and road maps coming from this Mandate have been aligned with existing work, especially research projects.

2.3 European standardization

CEN, CENELEC and ETSI are the official providers of European Standards and technical specifications. Their activities are set out by the Regulation 1025/2013 for the planning, drafting and adoption of European Standards and other deliverables in all areas of economic activity.
Standardization has a number of deliverables that are briefly described here.

European Standards (EN) are the principal product of CEN, CENELEC and ETSI. Developed by a Technical Committee, approved by their Members and featuring a public commenting stage in its development, an adopted European Standard is published as an identical national standard by the National Standards Bodies.

A standard is a publication that provides rules, guidelines or characteristics for activities or their results, for common and repeated use. Standards are created by bringing together all interested parties including manufacturers, users, consumers and regulators of a particular material, product, process or service. Everyone benefits from standardization through increased product safety and quality as well as lower transaction costs and prices.

Standards are a key component of the Single European Market. Although rather technical and often unknown to the public and media, they represent one of the most important issues for businesses. Standards are crucial in facilitating trade and hence have high visibility among manufacturers inside and outside Europe.

A standard represents a model specification, a technical solution against which a market can trade. It codifies best practice and is usually state of the art.

European Standards are based on a consensus which reflects the economic and social interests of the CEN Member countries channeled through their National Standards Bodies (NSBs, or equivalent national recognized organizations). Because of the 'all parties concerned' principle, all stakeholders can be involved in the standardization process. Referring to standards within a legislative text is viewed as a more effective means of ensuring that products meet the essential health and safety requirements of legislation than the writing of detailed laws. This allows both processes to support each other, without causing a slowdown. The European standards published by ESOs have a unique status since they also are national standards in each of its 33 Member countries. With one common standard in all these countries and every conflicting national standard withdrawn, a product can reach a far wider market with much lower development and testing costs. ENs help build a European Internal Market for goods and services and position Europe in the global economy.

In essence, European Standards relate to products, services or systems. Today, however, standards are no longer created solely for technical reasons but have also become platforms to enable greater social inclusiveness and engagement with technology, as well as convergence and interoperability within growing markets across industries.

By initiating standardization parallel to research projects, agreements on security, sustainability etc. become available as early as possible and therefore can be implemented faster.

It is important that standardization becomes more known in the security sector, which is one of the general results of this project, so that all stakeholders can benefit from the advantages standardization has.

It is possible that some of the proposals will need pre-normative research. It is also related to on-going research activities like FP7 and in the future Horizon 2020 as standardization can be of benefit in the innovation process and should therefore be involved in many research projects for the beginning. CEN is closely working together on this with the Joint Research Centres of The European Commission.

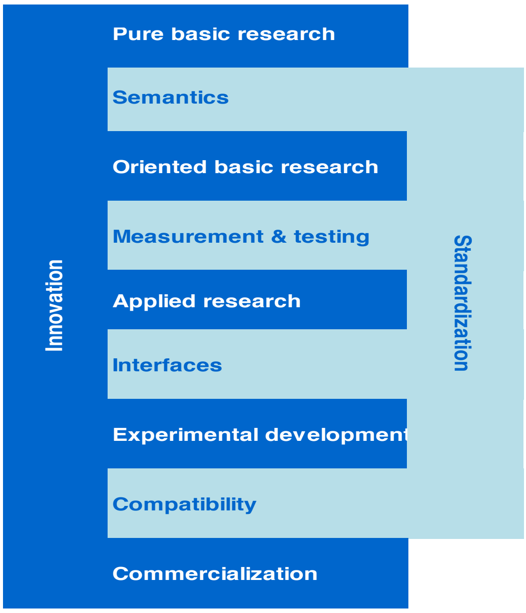


Figure 3- Benefits of standardization to innovation

Besides European Standards (EN) itself, other standardization deliverables can be developed quickly and easily within CEN: Workshop Agreements, Technical Specifications, Technical Reports and Guides.

CEN Workshop Agreements (CWA) are developed in CEN Workshops open to anyone with an interest in the development of the deliverable.
There is no geographical limit on participation and hence participants may come from outside Europe. The development time of a CWA is on average between 10-12 months. CWAs do not have the status of a European Standard and there is no obligation for the National Standards Bodies to adopt them as national standards.

CEN Technical Specifications (CEN /TS) can be used by CEN Technical Committees as a European Pre-Standard for innovative features of upstream technology, or when various alternatives need to coexist in anticipation of future harmonization. As with the CWAs, TSs do not have the status of a European Standard and are not adopted as national standards.

CEN Technical Report (TR) is an informative document that provides information on the technical content of standardization work. It may be prepared when it is considered urgent or advisable to provide additional information to the CEN national members, the European Commission, the EFTA Secretariat, other governmental agencies or outside bodies and there is a lack of time to develop an EN-standard.

Timeframes:
Each of those different types of documents has its own time-schedule.

Timeframe for the development of an EN - standard
The deadlines for the main steps in the process are mentioned in the table below, where t_0 is the date of registration of the active work item.

Step	Deadline
Dispatch of Enquiry draft to CMC	t_0 + 12 months
Submission to Enquiry	t_0 + 14,5 months
Closure of Enquiry	t_0 + 19,5 months
Dispatch of Formal Vote draft to CMC	t_0 + 27,5 months
Submission to Formal Vote	t_0 + 31 months
Closure of Formal Vote	t_0 + 33 months
DAV/Definitive text available	t_0 + 36 months

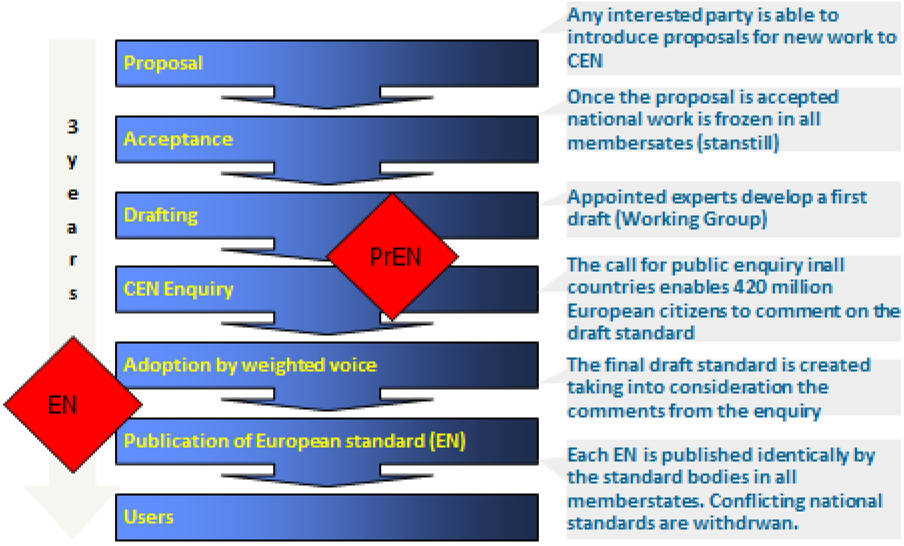
Table 1: Time frame development EN-standards

Timeframe TS and TR

The deadlines for the main steps in the process are mentioned in the table below, where t_0 is the date of registration of the active work item:

Step	Deadline
Dispatch of draft to CMC for submission to approval procedure	t_0 + 12 months
Submission of draft to approval procedure	t_0 + 15,5 months
Closure of vote	t_0 + 18,5 months
DAV/Definitive text available	t_0 + 21,5 months

Table 2: Time frame development TR and TS – documents


3 years
Proposal
Acceptance
Drafting
PrEN
CEN Enquiry
EN
Adoption by weighted voice
Publication of European standard (EN)
Users

Any interested party is able to introduce proposals for new work to CEN

Once the proposal is accepted national work is frozen in all membersates (stanstill)

Appointed experts develop a first draft (Working Group)

The call for public enquiry inall countries enables 420 million European citizens to comment on the draft standard

The final draft standard is created taking into consideration the comments from the enquiry

Each EN is published identically by the standard bodies in all memberstates. Conflicting national standards are withdrwan.

Figure 4- Development EN - standard

3 Results

3.1 General conclusions

Standardization is quite a new phenomenon in security industry in Europe, although it can be of great benefit for all stakeholders involved. For other industries that widely apply standardization, research has shown that every EURO invested in standardization yields about 10 to 100 EURO (Berger Institute).

Standardization and the benefit of it have been recognized by the European Commission since many years (see e.g. Regulation 2252/2004 and 810/2009 of the European Union). Therefore it seems only logical that being willing to give a push to the European security industry means investing in standardization.

Consequent to Mandate M/487, this report is a first step in a process that should lead to a standardization landscape in the field of security that will be of benefit for the industries involved and contribute to the security of EU citizens and residents.

Several common threats emerge from the report and these can be summarized as follows:

- Confidentiality – special attention is required in to standardization on security.
- Integrity on behalf of all stakeholders.
- Risk based work – ISO 31000 is a widely accepted standard in the sector.
- Terms and definitions – clear definitions are needed.
- Standardization and innovation – innovation can benefit a lot from early standardization.
- Timeline- proposals need to be prioritized and the roadmaps are only the start of a development.
- EU-policy – standardization in the security sector is an excellent tool to support EU policy.
- Reactions of stakeholders – stakeholders were generally positive about the mandate and participated actively.
- The need to meet the EU objectives and criteria through consideration by experts.

Confidentiality
One of the problems that stakeholders address when it comes to standardization in the field of security is confidentiality. As standardization is an open and transparent, consensus driven process, it is sometimes difficult to appreciate how it could contribute to making society more secure since classified information should not be openly accessible since it could assist criminals and terrorists.

European standards (EN) and other deliverables (see 2.3) can **not** be confidential. However for military or business reasons an open standard can be combined with a confidential annex solely for the purpose of work by military organizations or special businesses. CEN TC 391 initiated talks with NATO to declassify NATO standards in order to realize that useful work becomes available to all users.

Openness/ loyalty to the principles of standardization
There is one important thing that should be mentioned in the whole process of standardization, but maybe also in a wider context – that is integrity. Without integrity, security standardization or standardization in general is not possible. Of course, all stakeholders have their own agenda, but in the end it is the will to gain consensus that makes standardization and cooperation in general possible. It is also clear that

stakeholders gain more from participation than they would have achieved if they had tried to solve a problem on their own.

Risk based approach

A risk-based approach has been the starting point for the proposals in this report. This because experience has shown that whatever model is used, the determination of risk is always part of the analysis. ISO 31000 'Risk management' has proven its value since its publication in 2009 and there is a trend that all management standards in the sector are based on this standard.

Terms and definitions

There are several definitions of the words security and safety. It is a challenge to make a good distinction between safety and security. In some of the EU languages, safety and security are the same or almost the same.

In addition, related definitions such as crisis management, emergency management and resilience have different definitions in different countries.

It is not surprising than that all the experts that participated to this report have mentioned one specific need: to develop a common language within the selected sectors. In this report, no definition of safety or security is given. However, here safety is used as the umbrella for the technical aspects including technical failure. Security is 'the rest' including intentional and unintentional aspects. It will have to be part of the follow-up to develop the common language. There have been some efforts to harmonize all terms and definitions for security like the terms and definition standard in ISO (ISO 22300), in biometrics (ISO 24779 and ISO/IEC 2382-37:2012) and the CBRN glossary in Europe. However, even within ISO there are contradicting definitions.

Standardization and innovation

During recent years standardization has proven its value not only for products and systems that have been in place and use for several years, but also for innovative new products and systems. Those can benefit much from including standardization in the process of development as market introduction becomes much easier if one can prove that a product meets certain requirements when it enters the market. The European Commission has adopted this for many years, and many projects that are carried out within the research agenda Framework 7 (FP7) include standardization form the beginning. All stakeholders recognized the importance to the work in line with the future Horizon 2020 research program.

Not only the development of standards and methodologies in the field of the security industry is important, training of the end users, those who will bring those standards and methodologies in practice, is also an important issue. To ensure that all the end-users are educated in the same way, it is to be considered to develop training standards on the various subjects.

Timeline

For each workshop, proposals were invited, discussed and prioritized (see 2.2). For the roadmaps, proposals have been chosen as priority that have the most impact in terms of benefit for industry and better security and can be developed on short term.

EU-policy (implementation)

It is evident that in the security sector not only industry and the public are major stakeholders, but also policy makers. In the New Approach (see http://www.newapproach.org/) standardization is an important tool for policy makers as they set the (performance) requirements, and standards describe how these can be measured or proven. It is therefore evident that the roadmaps have been developed in cooperation with staff of several Directorates of the European Commission, as these roadmaps should support European policies and programs such as Horizon 2020.

Reactions of stakeholders
This report has been widely spread for comment amongst stakeholders. More than 350 comments on the draft version of the report were received. The outcomes of the workshops are the opinion of those who participated and therefore are given in the report, but all stakeholders had the possibility to forward their ideas and comments to improve the report. This, to make it easier for the EC to judge what proposals have the most support and the most impact.

The workshops were evaluated and the participants were positive about the way the workshops and the process were organized.

Meeting the EU objectives and criteria by expert judgement
All participants at the workshops were invited to give their opinion on why the proposals were going to meet the EU objectives and criteria.
The results were judged by the three experts and discussed with a number of stakeholders in interviews and the results of this expert judgement is given in a table for each of the three priorities of the Mandate M/487.

There are some general results found during the project:

1. Standardization, both the deliverables and the process, are not well known in the security sector. This is something that should be changed as all stakeholders that were involved in this project underline the importance of standardization and the potential benefit the security market in Europe and worldwide can have using standardization.
2. Interoperability and communication were two very important items in all interviews and workshops. Therefore this should also be one of the priority things looked at via standardization.

3.2 Results of the Border Security Survey

3.2.1 General

The emphasis in Phase 2 is on Automated Border Control (ABC) and this area of border control figures significantly in current standardization work, particularly in biometrics. Therefore the report concentrates on this subject.

The term for self-service passport control using biometrics and passports and/or tokens is generally agreed to be ‘automated border control’ and not ‘*automatic* border control’. In very few cases is ABC a totally unsupervised system.

It is also generally agreed that ABC systems can only be used by those in a recognised eligibility group: these might be those passengers who have pre-enrolled and received approval to take part (e.g. the UK *IRIS* system, Netherlands *Privium* and systems in the Middle and Far East); or passengers whose nationality and possession of an electronic machine-readable travel document (e-MRTD) allow them to cross borders with no further formality (see for more information http://www.frontex.europa.eu/assets/Publications/Research/Biopass_Study.pdf).

See also Annex B.3 for an overview of ABC.

The overall picture of *standards and recommended practices* for automated border control resembles a somehow incomplete jigsaw puzzle.
The majority of the pieces are already in place and one can discern the overall picture. Thanks to published standards for passports and identity (ID) cards, i.e. the machine readable and electronically enhanced variety (ICAO 9303) and the biometric modalities associated with them, the requirements and specifications for ABC in Europe and across the world are already very similar and are constantly converging.

There are a number of 'components' which make up a working ABC system, most of which can be subject to standards (see also Annex B.1):

- Passengers.
- Supervising border agency staff.
- Operational and fallback procedures.
- Eligibility rules.
- User familiarisation.
- Travel documents and tokens.
- Travel document data capture devices.
- Biometric capture devices.
- Biometric matching techniques.
- Barrier mechanisms and sensors.
- System logic.
- Data interfaces.
- Business case, societal issues and system design methodology.

3.2.2 Current Standardization Landscape

The work of ISO/IEC JTC1/SC37 (biometrics) is continuing and ABC and other identity management applications are often used as examples or subjects of technical reporting.

The European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex) has produced some excellent high-level guides to the technology and operation of ABC.

CEN TC/224 (WG18) is currently working on technical specification (CEN/TS 16634) for biometric ABC systems, though a number of the issues discussed in this document are out of its scope:

"This TS primarily focuses on biometric aspects of Automated Border Control (ABC) systems. Drawing on the first European and international ABC deployments, it aims to disseminate best practice experiences with a view to ensure consistent security levels in European ABC deployments. Furthermore, the best practice recommendations given here shall help make border control authorities' processes more efficient, speeding up border clearance, and delivering an improved experience to travellers.

ISO/IEC has published a series of standards dealing with biometric data coding, interfaces, performance tests as well as compliance tests. In order to promote global interoperability it is essential that all these standards are applied in European deployments. However, these standards do not consider national or regional characteristics; in particular, they do not consider European Union privacy and data protection regulation as well as European accessibility and usability requirements [7]. Thus, this Technical Specification amends the ISO standards with respect to special European conditions and constraints.

The TS systematically discusses issues to be considered when planning and deploying biometric systems for ABC and gives best practice recommendations for those types of systems that are or will be in use in Europe. The document deals with personal identification including ergonomic aspects that have an impact on the acquisition of biometric data.

Communication, infrastructure scalability and security aspects other than those related to biometrics are not considered. This document also does not consider hardware and security requirements of biometric equipment and does not recommend general border crossing procedures.

The enrolment process, e. g. for electronic passports, is out of scope of this document."

CEN also plans further work on environmental influence for operational deployments of European ABC systems and mobile ABC systems.

3.2.3 Stakeholders

Organizations such as the International Standards Organization (ISO), the European Committee for Standardization (CEN), the International Civil Aviation Organization (ICAO), the US National Institute of Standards and Technology (NIST) and the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex) are all active in both the technology and operation of ABC systems and have filled in much of the standards and recommended procedures picture.

Stakeholder Analysis

The identified stakeholders in ABC systems include:

- Users of the system – passengers, crew and port staff passing through a border check.
  Passenger users are not-ABC-experts and generally not aware of standards. They are impacted however by lack of standards, either through initial inability to use the system through insufficient training or by using different systems in different locations.
- Users of the system – border agency staff supervising the ABC system.
  Staff using the system need well-designed interfaces and clear operating instructions. The former is the responsibility of the supplier, the latter that of the operator.
- Users of the system – government staff with responsibility for border control policy, law-enforcement, intelligence etc.
  Customers of ABC should be able to expect that specifications from different suppliers will meet international standards so that evaluation and selection of supplier is easier and fairer.
- System managers and maintenance staff.
- Suppliers of complete systems and components.
- Agencies and individuals responsible for, or concerned about, data protection and privacy.
- Governments, academics and commercial entities involved in research and development.

- Those concerned with health and safety issues.
  Adherence to international safety standards aids type-approval and certification
- Those concerned with issues of equality and diversity.
  ABC systems should be the same for all eligible passengers and standards can assist in determining which passengers should use adjusted ABC systems and which should be offered alternative procedures (e.g. people in wheelchairs)
- Agencies owning or managing port environments and their trade associations.
- Passenger carriers and their regulatory or trade associations.
  Airports and carriers are in a competitive market and where they are obliged to invest in ABC or similar devices (such as electronic/biometric self-service devices) then they demand a 'level playing field' where impact is spread evenly across them
- Designers, producers and issuers of travel documents.
  Standardization ensures that passports can interact effectively with any ABC device and can be authenticated and their electronic data verified
- Creators and managers of standards and best practice related to ABC

3.2.4 Workshop

Delegates debated 64 proposals, which they had submitted prior to the workshop, clarified them and reduced them in number, at the same time ranking them in order of priority for further action (see chapter 2.2 for explanation of the priorities).

The broad range of proposals received before the workshop was divided, arbitrarily, into four categories in order to facilitate consideration by two groups of delegates over two sessions. The level of expertise in the groups was high. Each topic was discussed and ranked into four levels of priority (see 2.2) and a separate level of 'out of scope/unranked'.
Some of the proposals were suggestions for system features rather than standards.

The conclusions of the workshop were recorded, summarised and then disseminated to both the workshop delegates and a wider selection of stakeholders by email for validation and comment.
In addition, each stakeholder group and each physical and logical component of an ABC system was considered to determine whether international, European, national or commercial standards applied. A check was also made of work in progress by standards bodies affiliated to ISO/IEC and CEN.

Reference was also made to technical literature and internet resources of manufacturers.

3.2.5 Standardization roadmaps

The problem is not so much that standards for components of ABC are missing but that they are not well known or mandated in procurement documents. This is mainly because:

- Customers are not aware of them and therefor do not insert them into system requirements;
- Suppliers and integrators do not yet see advantage in formally complying with standards because customers do not ask for them;
- Some standards and recommended practices are not yet out of drafting phase;
- Some excellent and relevant ABC guidance does not have 'standard' status but these guidelines require additional resources to transfer into international standards;

- When quoted in specifications or procurements, the requirement to adhere to a particular standard is stated in the general without an indication of which parts are relevant;
- The absence of biometric standards profiles relevant to ABC systems.

The advantages of a full set of up-to-date, accessible and pertinent standards for ABC in Europe and worldwide are as follows:

- They provide a common reference point for discussions between parties about safety, performance and quality;
- The need for extensive evaluation is reduced as conformance with documented specification can be assured;
- ABC systems in the same geo-political area are more likely to be common, compatible and interoperable;
- Certification and quality control can be formalised to ensure continuing performance;

A recent consultation with experts in the field of biometrics, border control technology and border management (as part of this study) did not reveal any serious gaps or defects in the ‘standards landscape’, rather the response was to consolidate existing standards and practices into documents more accessible to the ABC community and to fill in the remaining gaps.

The European Union aims by the end of this decade to introduce a common border control system (’Smart Borders’, aimed at using new technology to speed-up, facilitate and reinforce border check procedures for foreigners travelling to the EU) which will rely extensively on ABC system to handle border crossing by both EU citizens and non-EU resident and regular travellers. To ensure commonality, compatibility and interoperability of ABC systems in individual Member States the *standards jigsaw* needs to be completed.

The recommendation for border control is therefore consolidate existing standards and practices into documents more accessible to the ABC community and to fill in the remaining gaps.

The European Commission and Frontex as well as CEN/TC 224 and CEN/TC 391 are invited to consider several proposals.

Missing standards

Gaps that have been found are:

- Standards and recommended practices for passenger and operator health and safety in automated border control systems.
- Data protection and privacy.
- Passenger education and familiarisation.
- Performance testing of ABC – standard methods of timing transactions, assessing biometric decision thresholds
- Effective certification of ABC systems. Performance of individual gates as a result of environmental aspects (ambient light, temperature, humidity etc.).
- Standards for performance can be checked and systems certified as compliant.
- Accessibility for less-abled passengers.
- Anti-evasion, anti-spoofing and security sensors.
- A standard set of specifications to allow certification of ABC systems.
- Standards and recommended practices for border guard monitoring of ABC systems.

- Common functionality for ABC – data exploitation, watchlists etc., document examination
- Standards or recommended practices for business cases, project management methodology for ABC systems to enable faster, less risky procurement and implementation.
- Security of ABC systems against hacking, infiltration and corrupt practices.
- Travel document issue procedures and standards, registered traveller enrolment.

Proposed standardization roadmaps with work programme:
In the next table, the priority 1 proposals from the workshop are grouped into six groups and the lower priority proposals are mentioned within each of them.

To fill in the blank spaces in the international standards jigsaw, both CEN/TC 224 and CEN/TC 391 are recommended to consider a number of areas and to turn whatever documentation exists into workable European standards.

Proposal	Priority [(1)]	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
Priority One Roadmap Projects – Determining Strategic Design of EU ABC Systems: Safety, Privacy, Security and Accessibility							
1 A set of consolidated standards and, if necessary, recommended procedures to protect and promote the health and safety of passenger and staff users of European ABC systems.	1	EN, TR, CWA		Hardware objects (eg moving doors, machine cabinets), radiating devices (eg electro-magnetic waves), physical bodily movements and mental effort characteristic of ABC systems should not cause harm to passengers and staff or damage to their property. The proposal should include lower priority issues such as standard emergency procedures (fire, evacuation, trapped passengers etc), alarm devices etc	Individual components should comply with relevant existing standards or comply with standards introduced because of this work. Effects could range from trivial to severe, depending on the design of components.	Border control agencies should procure and implement only compliant systems; suppliers should offer only compliant components passengers will be protected against foreseen harm whenever they use ABC.	FP7: FastPass; EFFISEC IATA:Checkpoint of the Future Dialogue with these projects will inform the standardisation process in terms of practicality and effectiveness
2 A set of consolidated standards and/or, recommended procedures to protect and promote data protection and privacy for European ABC users.	1	EN, TR, CWA		The amalgamation of large amounts of 'personal data' (as defined by legislation) and biometric data (mainly face, fingerprint and iris) across Europe makes common data security and security policies and procedures much more necessary to preserve public confidence in ABC systems.	Enable suppliers and operators to more confidently adhere to European data protection and privacy legislation by building products and services using 'privacy by design'	Border control agencies and port operators classed as data owners and data processors. Deliverable should apply to all new systems and upgrades.	FP7: FastPass; EFFISEC; FIDELITY IATA:Checkpoint of the Future Dialogue with these projects will inform the standardisation process in terms of practicality and effectiveness
3 A set of consolidated standards and/or, recommended procedures to promote passenger and operator familiarisation with European ABC systems at the point of interaction.	1	EN, TR, CWA		Passengers are still largely unaccustomed to navigating ABC systems (unlike automated teller machines (ATM)) and it would be highly desirable for the user experience to be the same globally. A guidance document would be useful in	Suppliers will be obliged to comply with such standards/recommended practices when designing warning and advisory information.	Border control agencies and port operators which operate ABC systems.	FP7: FastPass; EFFISEC; FIDELITY IATA:Checkpoint of the Future Dialogue with these projects will inform the standardisation process in terms of practicality

Proposal	Priority [1]	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		EN, TS, TR, CWA		Why is this an important proposal?	What will be the impact of the deliverable, especially for industry?	Who will use this deliverable, for what aim and how often will it be used?	What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?
				ensuring that publicity, audio/visual instruction for both passenger and border agency users was standardised, much in the same as in-flight safety information is standardised.			and effectiveness
4 A set of consolidated standards and/or recommended procedures for the evaluation of performance of European ABC systems eg transaction times, biometric system accuracy in business environments. A standard set of specifications to allow certification of ABC systems. A set of standards and/or recommended practices for evaluating the need and specification for new or replacement ABC systems	1	EN, TR, CWA		The transaction time and accuracy claims by ABC suppliers can be based on different calculations and assumptions with the result that potential purchasers may not be able to make valid comparisons or understand the basis of the claimed performance. The proposal should also include standards for ABC resilience in varying environmental conditions (light, temperature, humidity, wind-chill, dust, salinity etc) The proposal should also include standards for recommended practices for business cases and requirements/specifications and stakeholder engagement on new ABC projects to ensure a high likelihood of the project delivering the expected benefits.	Suppliers obliged to calculate performance figures (e.g. transaction times) according to an agreed algorithm so that competing systems can be compared using practical, real-life metrics.	Suppliers of ABC system components and systems	FP7: FastPass; EFFISEC IATA:Checkpoint of the Future Dialogue with these projects will inform the standardisation process in terms of practicality and effectiveness

Proposal	Priority [1]	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
5 A set of consolidated standards and/or recommended procedures for accessibility to European ABC systems for less-abled passengers which supplement Member State national legislation.	1	EN, TR, CWA		To promote dignity and equality of citizens and other nationals using EU systems.	'Reasonable adjustments' to components and/or the implementation of ABC systems such addition of larger displays or widened access lanes.	Designers, suppliers and ABC implementers	FP7: FastPass; EFFISEC;CARDIAC IATA:Checkpoint of the Future Dialogue with these projects will inform the standardisation process in terms of practicality and effectiveness
6 A set of consolidated standards and/or recommended procedures for anti-evasion, anti-spoofing and security sensors performance and reliability.	1	EN, TR, CWA		There is not yet a standard set of tests or levels of resilience for biometric, electro-magnetic spectrum and mechanical devices which are designed to detect abnormal behaviour in ABC transactions. ABC systems should have standards and/or recommended practices for digital security (digital certificates from RFID security), public key directory etc.	Performance of security features in ABC systems will have to meet higher standards and be consistent and more rigorously tested.	Designers, suppliers and ABC implementers	FP7: FastPass; EFFISEC; FIDELITY IATA:Checkpoint of the Future Dialogue with these projects will inform the standardisation process in terms of practicality and effectiveness

Table 3: Priority One Roadmap Projects – Determining Strategic Design of EU ABC Systems: Safety, Privacy, Security and Accessibility

[1] The Roadmap Projects with priority 2, 3 and 4 can be found in Annex B.2

A suggested work programme for ABC standards and recommended practices is shown in the figure below. Areas of work with the most impact upon suppliers and operators are shown towards the top of the diagram, priority towards the left. The priorities should be to increase the security and integrity of ABC but also to increase its acceptability and ease of use for passengers. Other issues, such as the safety of ABC installations and accessibility are already covered by existing regulations, but not in a pan-European consistent manner.

A high level of a work programme is shown in the following figure:

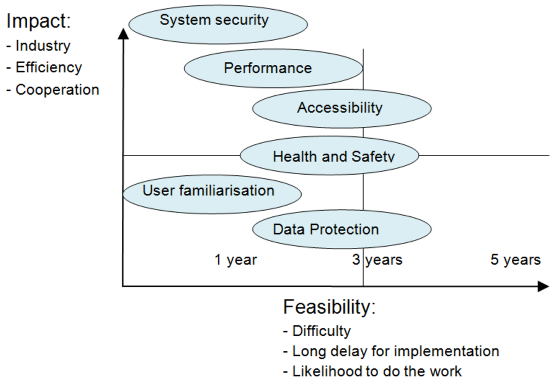


Figure 5: High level work programme Border Security

3.2.6 Results and recommendations

During the period of this project a number of workshops and meetings related to biometrics and ABC systems were attended:

- ISO/IEC JTC1/SC37 committee (in Winchester, UK);
- British Standards Institute (BSI) IST/44 committee (at their Chiswick, London HQ);
- Biometrics Institute (Biometric Vulnerability seminar in London);
- CEN (in Brussels);
- Frontex ABC meetings (in Helsinki and Sofia);
- FastPass project meetings and workshops (in Vienna and Helsinki)

This was to determine the progress of standards and technical reports in the field of biometrics – the science that enables ABC systems – and operational ABC guidance.

There is a very strong emphasis on ABC and border control security in these works streams: ABC and border security are among the first adopters of biometrics and ABC figures frequently in work group activities.

The range work covers rigorous technical standards for biometric modes and the related technology, conformance testing, as well as operating practices, selection of equipment and solutions and the use of biometrics by children and people with disabilities.

Frontex has also produced some excellent and very detailed documents on the technical requirements and operation of ABC systems.

The European Commission is sponsoring research & development in border control technology, most notable the FastPass and EFFISEC projects. Both aim to produce in the next few years standard border facilitation and protection prototypes that will in turn both update standards and generate new ones. The EU Framework 7 FIDELITY programme is looking at improving the security and integrity of electronic machine-readable travel documents, an essential component of ABC.

Taken together, this represents a comprehensive, detailed and almost complete picture which will improve over the next four to five years. The task was to determine where there were missing, outdated or defective standards and recommended practices.

Generally, European/international standardization work and harmonisation has to have priority. The development of European standards, as proposed in this report, intends to complement international standards or to meet special European requirements only as far as necessary.

Recommendation 1
Raise awareness of international standards for the specification and operation of safe, secure and cost-effective ABC systems amongst the key-stakeholders; the operators of systems, the supplier community and regulatory authorities, and to consolidate relevant aspects in a form which is accessible to, and usable by, all of them.

In order to achieve this aim, the European Commission and Frontex should ask CEN to work with ISO/IEC Joint Technical Committee 1 (JTC 1) subcommittees SC37 on biometrics and SC27 on security to create a definitive guide to ABC specification and design. The final version of this text should be in place before individual authorities start specifying equipment and systems as part of the EU's 'Smart Borders' initiative.

Recommendation 2:
In order that the work programme outlined below is delivered, the European Commission is requested to make available suitable resources, since lack of funding was mentioned as important reason for delay by the stakeholders.

Recommendation 3:
CEN is advised to consider updating existing standards on human-computer interaction and on the safety aspects of ABC systems – for example folding and sliding glass doors, fire and electrical safety, egress in *emergencies*, blast damage resistance.
These are often covered in standards (e.g. software design and building construction) not obviously linked to ABC.

Conclusion
Organizations such as ICAO, NIST and ISO have done much to create standards and recommended practices for the components of ABC in the last ten to fifteen years. The documents created by these bodies, plus the very useful and detailed recommended practices produced by ICAO and Frontex should to be much better known and used.

There remains to be some consolidation of standards pertinent to ABC and some work to be done around the safety and performance of ABC components

As well as the rigorous technical standards for ABC components, there needs to be standardisation of ABC as a whole – *in the way it is used*, not just in the way it works.

3.3 Results of Crisis Management:

3.3.1 General

Crisis Management is understood here in broad terms, i.e. the organization, processes, coordination and response drive to crisis, from natural, technological or malevolent origin, including cyber-crisis or even financial crisis, which would profoundly affect health, safety, security, economic or social well-being of the citizens.

Crisis management implies **networking and communication** with all the stakeholders and the general public. As a result, **interoperability** is critical to facilitate these communication needs. It is all the more difficult during a major crisis, when there is a strong cross-sector, cross-border, cross-hierarchy coordination need.

Crisis Management is a **complex field**, because it involves many stakeholders, from many organizations, with different objectives, procedures and reporting structures and often different definitions of all aspects of crisis management. It also involves the general public, would it be on the victim side, on the warning side or just involved in rumour generation that can help but also can create a lack of trust or confidence. Crisis management is using integration of technologies, human elements, training, behaviour, etc. We are not yet at a stage where we can interconnect information management systems from different organizations to share situation assessment or automate coordinated response procedures. For many reasons (political considerations, concern about the confidentiality of the information, competition or conflicting objectives between organizations, human behaviour, lack of financing, etc.) there is no willingness to establish direct interconnection, but rather a need to utilise human interfaces between systems (i.e. liaison officers between organizations). This understanding means that technical solutions should be incremental solutions, in a step by step approach, as enablers of communication needs, and require training and experiments.

Crisis Management necessitates doctrine, procedures, organization and responsibilities definitions of public agencies that are under **Member State** control, through the national legal frameworks and guidelines, in application of the subsidiarity principle. As a result, no major standardization in this area can be done without the Member States' cooperation. Member States are very cautious, even more when there is recommendation for certification which is perceived as contrary to the rights and the sovereignty of the States.

In this regard, **marketing of standardization** work is of upmost necessity. Many participants in the workshop had no idea of existing work.
In addition, crisis management practitioners see standardization only through dissemination of centrally produced guidance material.

Lastly, a close collaboration with all relevant standardization committees and initiatives is required to avoid duplication and foster synergy, while Europe would lead some of the recommended standardization proposals, and CEN/TC 391 serving as a facilitator.

3.3.2 Standardization needs

Crisis management is considered in a broad sense to encompass all types of crises, including natural and man-made disasters, financial crisis, cyber crisis or terrorism crisis and more generally all types of crises that would profoundly affect health, safety, security, economic or social well-being of the citizen. A particular attention was given for major crisis because the criticality and the spread of the situation require a stronger need for coordination between different organizations, different activity sectors, different hierarchical layers of command and control, and different Member States. As a result, interoperability concern is confirmed to be critical to crisis management, all the more for major crises.

This does not imply that crisis management standards should be considered only during those major crises. On the contrary, standards make sense only if they are utilised for regular activities and minor crises, and embedded in operational systems and approaches.

Standardization activity concerning interoperability for crisis management is not the only way to achieve improvement in European security industry, in crisis management efficiency and effectiveness or in coordination or cooperation at the European level during major crises, but it can contribute to it. Proposals from the workshops that are not selected at the present time for future standards, can still be very useful for technical specifications or working group activities, particularly concerning good practices, and contribute to set the foundation for further research activities (i.e. under the Horizon 2020 research program).

A last important element, which was mentioned during the workshop and interviews, is the importance of human aspects. Crisis management is primarily the capacity to coordinate many human actions, to share situation assessment, to make, implement and control coordinated actions, and to adapt the response to changing situations. As a result any information system interoperability will have to consider human action or human liaison in between systems, before considering a possible long term objective of integrating organizations specific systems. In this regard, crisis management interoperability is quite different from, as an example, supply chain interoperability. In addition the human aspect is also critical when one looks at communicating to the general public, obtaining trust and confidence, avoiding false rumours in e.g. social media and managing the psycho-social elements during the crisis and when returning to normal.

Need for semantic and organizational standardization.
To better understand and distinguish between different concepts and facilitate communication and understanding (before, during and after crises) there is a need for a vocabulary and generic models. These ‘quick win’ actions can be subdivided in several projects, in priority order:

1. There is a need for a high level overall presentation and clarification of relationship between management systems :
   - Risk management.
   - Activity continuity management.
   - Crisis management.
   - Resilience management.

This action is considered vital to get major stakeholders understanding and acceptance of standards.

2. Semantic interoperability is needed for basic concepts:
   - Risk manager.
   - Crisis, Major Crisis, Cross-sector crisis, Emergency, Disaster, incident/risk classes.
   - Resilience.
   - A glossary comprising at least the most important European languages would be strongly appreciated in addition to the vocabulary list of ISO 22300 to facilitate communication

The objective is not so much to make new definitions, but to match existing ones to make sure people understand each other, even if they are using different languages.

3. Semantic interoperability is needed to make communication possible between users of different Emergency Management Systems, by providing mapping among different classifications at both national and international levels for some commonly used map objects (icons and terms).

4. One step further would be to utilize a set of minimum semantic map objects agreements and minimum standardized icons to establish a common geospatial basic information system, based on Geographic Information Systems (GIS) standards, to be used by organizations before and during crisis situations (it will allow these organizations to provide additional information to the common base or to retrieve information from the common base that they could consolidate within their own systems). This geospatial standardization work could also include geospatial information for underground facilities and buildings. This is an urgent need to facilitate all emergency activities indoors. All this work would eventually evolve later towards a more developed meta data reference.

5. Organizational interoperability is needed to understand the organizational structure of command and control (C&C). The proposal is to establish a C&C reference model, with a generic description of missions, responsibilities, functions, structure, for the different hierarchical layers, together with a semantic model and interfaces with the outside world (general public, NGOs), not to serve as a standard but to facilitate :
   - sharing a common cross-border definition of commonly used terms within one organization or one country (i.e. definition of the hierarchical structure that is using today different wordings such as strategic, tactical, operative, or gold, silver, bronze, that are not well understood);
   - mapping of organizations hierarchical levels and responsibilities within Member State (MS) and between MS;
   - establishing direct contacts at the right levels that would allow knowing the people, exchanging liaison officers and identifying the types of information to exchange;
   - coordination in a cross-border, cross-sector, multi-hierarchy, public and private context, for situation assessment, response decisions and communication policy to the public. Priority will be given to top layers communication needs, because it is easier at this level to make abstraction of existing constraints generated by specific organizations and reporting procedures.

These activities will capitalize on FP7 projects.
They will also facilitate work on good practices identified during the workshop, and very useful for people in charge of crisis management, such as:

- differentiate the vertical layers in different countries, with roles and responsibilities prior to any crisis.
- develop coordination at the strategic level for complex cross-sector, cross-border major crises.
- develop procedures for collaboration and close interoperability gaps in international crises and disaster response.
- improve the management of vertical bottom-up information flow for situation assessment, both within the public sector and within private organizations to facilitate and accelerate real understanding of key issues, identify critical information or priorities and to facilitate the capacity to anticipate the situation evolution by the transmission of appropriate information based on a better understanding of next layer expectations.

- improve decision support system and situation awareness by information filtering & delivery for top level organizations.

Need for guidance in crisis response planning.

To facilitate interoperability there is a need for guidance in crisis response planning.

Some actions can be "quick wins", other may take more time, but all are useful to increase efficiency and effectiveness in response practices and coordination between MS.

1. Basic emergency response principles should be revisited to facilitate interoperability in emergency response planning, including the points developed underneath.

2. The linkage between response planning and the previous done risk based work, in order to optimize response efficiency must be reinforced.

3. The process to define the "limited key information" to share (pre, during, post incident) to improve preparedness, coordination and debriefing (between different actors and different hierarchical levels) must be standardized.

4. Coordination between command centres by developing common methodologies must be facilitated :
   a. for anticipation and decision making process under uncertainty (when there is a lack of information, unreliable situation assessment, uncertainty about situation evolution).
   b. for improving the process of incident qualification, escalation and warning decision.

5. The efficiency of pan European exercises (building on the existing work of ISO/FDIS 22398) must be improved to define EU exercises evaluation procedures: Crisis Management performance parameters, identification of gaps, identification of best practices, communication/planning/implementations of findings, development of lessons learned data base, in other words a production of a common identified lessons implementation process (identification, implementation, inclusion in e.g. training courses). A distinction should be made between evaluation procedures for exercises to test the planning process and exercises to test operational reactivity and agility.

6. A similar approach is needed for pan-European after crisis handling.

7. Training at a European level should be encouraged (table-top, simulation, operational). Training on how to run simple exercises (plan, execute and report) and to involve citizen, communities, and organizations with plans to increase community resilience. Multi-agency and common cross-border training programs (share best practices, networking, get to know each other, continuous improvement) should be encouraged.

8. Preliminary work could look at simulation needs to standardize some objects models (digital re-usable assets) for modelling and simulation environment (application for cross-boundary training). Standardization for building information with object models for the representation of both structural and functional aspects

of facilities. It would be useful for simulation of service deployment for transport system and for rescue personnel training.

Need for guidance for resilience.

This is a good example of a standardization action with motivated actors to work on it, in order to reinforce resilience capabilities.

1. We need a standard about resilience with good practices and concept for crisis management based on agility more than on planning. It should concern development of good practices, not requirements for certification. Such an approach is complementary to ISO 22301 (Business continuity management systems – Requirements). It concerns both agility during response phase and preparation for agility. It assumes a good understanding of the context (organization and capabilities).

2. This standard will also improve territorial resilience (first hour quick actions to undertake, fall-back pre-defined mode).

Need for developing improved reporting and mass warning systems.

This issue has to be developed for EU wide interoperability from the citizens perspective (improvement of the EU citizen experience). Several very specific actions are identified;

1. Standardize the way of acquiring digital information from victims/public and sending it to the whole command & control system (it may include developing a common 'victim ticket', to be filled in by victims using smart phone emergency applications).

2. Standardization of technical aspects of alerting:
   a. Develop client-based applications to decode alert messages in consumer receivers (smart phone, tablet, etc.).
   b. Specify the use of navigation enabled devices for alerting.
   c. Establish a standard way to refer to administrative areas with geo-codes that are valid all over Europe for alerting purposes.

3. Develop a common language for warning (alert and notification):
   a. Develop alert libraries that are applicable in all European countries (going beyond ISO/DIS 22324 on colour coded alert and ISO/DIS 22322 on public warning systems).
   b. Develop a communication protocol that allows lightweight transmission of alert messages and supports light encoding of the alert libraries; with possible use of wireless media (suggest more specific use of the Common Alerting Protocol (CAP), based on alert libraries, to allow interoperability).

Improve operational efficiency.

1. Assistance to first responders (localisation):
   a. Geo-localization (GIS) standards for use in buildings and underground systems to facilitate FR intervention. It concerns two standards (how to implement technology, such as the use of radio wireless communication protocols, and how to acquire the geo-localization information).
   b. Facilitate interoperability of unmanned search and rescue equipment.
   c. Standardization for providing dynamic information during an emergency (i.e. evacuation information in real time, location, infrastructure availability, exit routes availability).

2. Emergency management interoperability (detection):
   a. Standardization of detection equipment for search and rescue (to facilitate international missions).
   b. Activate distress beacon resource application for smart phones by victim.

3. Assistance to victims management:
   a. Standards on patient-management in mass casualty incidents (e.g. minimal data-set for patient-management in mass casualty incidents, management of data of affected persons in mass casualties, which shall duly take into account privacy issues and personal data equipment).
   b. To close the gap in (inter)national pre-hospital patient-management with differing national standards. Develop a standardized electronic triage system to improve the logistics and the situation awareness.

Awareness.

The workshop and the interviews with stakeholders show that awareness should be developed. Standardization should focus on raising awareness, because citizens and the community have to be aware of the risks

1. To reinforce citizen and local territorial community awareness and involvement, with increased knowledge of risks and available channels for information and advice for appropriate actions (before, during and after the incident)

2. Warning (alert and notification) dissemination understanding. Develop alert libraries that are applicable in all European countries. Define common European messages schemes for fire and evacuation systems. Capitalize on existing ISO/DIS 22322 on public warning process and ISO/DIS 22324 on colour coded alert.

Communication interoperability for command and control (C&C) centres

This topic is intentionally mentioned at the end of the list of proposals, because the market is not ready yet for systems interconnection. Different systems should be regarded as a fact of life; so interoperability is a must. However interoperability is assured today by human interfaces between C&C systems from different organizations (with different objectives, different sensitivity to information and different reporting structures). The same is true between public and private organizations. They are looking to improve common semantic, planning practices and cooperation at all hierarchical levels through liaison officers, but not for systems interconnections. One has to mention though that there are experiments, trials, demonstrations and even pilot projects of shared information infrastructure for security that can be precursors of more interconnected crisis management systems in the future.

The proposal is therefore to reinforce communication interoperability between command and control (C&C) systems. Communication interoperability could be improved by a better definition of needs and the use of minimum common terms/formats, information objects and minimum set of requirements. It will be implemented on a volunteer basis, considering the experience gained from existing implementations or projects. This work will eventually allow progressive standardization of event description and of digital objects, adaptation to evolving technologies and establishment of mechanisms to share information on a regular basis. This could lead to revisiting the work on shared situation awareness (e.g. ISO/DTR 22351and Tactical Situation Objects (TSO)).

This work should also contribute to previously mentioned needs:

a) To improve the management of bottom-up information flow for situation assessment, both within the public sector and within private organizations to facilitate and accelerate real understanding of key issues, identify critical information or priorities and to develop capacity to anticipate situation evolution.

b) To improve decision support system and situation awareness by information filtering & delivery for top level organizations.

Best practices.

A number of areas to improve and best practices to share that were not considered at first as relevant for standardization are listed here. The importance of these areas for efficiency of crisis management and coordination/cooperation during crises justifies considering some of them for standardization or Technical Specifications or Working Group considerations. Some of them are mentioned in previous paragraphs:

Incident management: first hour(s):	
	Use of social media. Early detection through weak signals. *Comments: This topic could easily evolve towards a standard on how to best detect, qualify and exchange (sometimes classified) information about early signals at a European level.*
	Methodology for sourcing information (social media, tweets, crowd source information) to assess impact of wide scale disaster and identify public needs.
	Communicating to the general public and avoiding wrong rumours.
	Develop smart phone emergency specific applications (situation reporting, CCTV capabilities, citizen as a sensor, etc.).
	Develop a common and standardized procedure in order to let citizens actively bring in their resources into the relieve effort (e.g. a 'resource ticket' available on mobile phones and the web).
C&C interoperability (Part 1, organizational interoperability):	
	Best practices in application of the generic organizational model: ▪ differentiate the vertical layers and clarify semantic. ▪ develop coordination at the strategic level for complex cross-sector major crisis. ▪ develop procedures for collaboration. • close interoperability gaps in international crisis and disaster response. • roles and responsibilities are clearly identified prior to any crisis. • clearer understanding of deliverables before, during and after the crisis. • deliver a set of common 'Business Protocols' across the area of communication.
	Creation of a centralized data base of events, decisions, following actions plans for memorizing all important information with their date, hour.

Table 4: areas to improve/best practices for reconsidering standardization

Further analysis:

The following topics were mentioned for further analysis; among them there are candidates for standardization.

Preparedness (simulation tools, training):	
	Standardization of objects models (digital re-usable assets) for modelling and simulation environment (application for cross-boundary training). Standardization for building information with object models for the representation of both structural and functional aspects of facilities. It is useful for simulation of service deployment for transport system and for rescue personnel training.
Operational efficiency:	

	Development of standards based on bottom-up identification of the minimum improvements expected hands-on by field staff (electrical plugs for generators, diameter of pipes, etc.).
C&C interoperability (organizational interoperability): good candidate for later standardization:	
	Improve the management of vertical bottom-up information flow for situation assessment, both within the public sector and within private organizations to facilitate and accelerate real understanding of key issues, critical information, priorities and to develop capacity to anticipate situation evolution by a better understanding of next layer expectations. Improve decision support system and situation awareness by information filtering & delivery for top level organizations
	To define standardised sets of meta-data for risk descriptions including co-ordinates, probability, severity, nature of the risk and possible triggers.
C&C interoperability (communication interoperability):	
	Facilitate information exchange between Crisis Management/Civil Protection and Critical National Infrastructure Operators

Table 5: Topics for further analysis

3.3.3 Workshop

About 60 participants in three workstreams discussed the more than 180 proposals:

- Workstream A to discuss possible actions to undertake before the incident to facilitate interoperability. It includes risk management linkage, planning methodologies, semantic, cross-border exercises and resilience.

- Workstream B to discuss interoperability issues during the reporting and warning phase and during first emergency response actions. The objective is to improve the EU citizen experience when located in a different Member State and improve interoperability from a bottom-up approach.

- Workstream C to discuss interoperability when the command centres are in place. The objective is to facilitate communication between the many actors concerned by crisis management, to improve coordination and efficiency in crisis response.

This workshop was very much appreciated by the participants and allowed prioritization of the proposals. More importantly the workshop showed that there is a momentum of stakeholders (from governments, private operators or suppliers of product or services) to work on interoperability for crisis management.

Interviews and workshop have shown some major areas for standardization (in a broad sense), either as new areas or extension of already existing areas, including technical reports or working groups and each one subdivided in specific actions.

It could be looked at in large functional domains, like the ones that were utilized during the workshop:

- Before the incident: Planning methodology, semantic, resilience.
- At the beginning of the incident: Incident reporting and warning using digital media and alert libraries.
- First response: First responders' practical tools to improve efficiency.
- During the crisis: Command and Control, organizational and communication interoperability, including coordination of communication to outside parties (general public, NGOs, volunteers).

3.3.4 Standardization roadmaps

Standardization is only part of the solution to achieve improvements in interoperability in crisis management. The current standardization landscape is already quite extensive (see Annex B.1, C.1 and D.1 for an overview in the different priority sectors) but further work is justified.

The workshop confirmed that standardization work for interoperability in crisis management should first consider semantic, planning, resilience and organizational interoperability issues, then some pragmatic technical and syntax aspects, with a bottom-up approach (looking at first responders needs and mass notification to the population), and lastly communication interoperability between command and control centres, as enablers of coordination and cooperation efficiency.

Future work in standardization should indeed consider in a first phase methodologies or general principles, and facilitate interoperability by providing common semantic and the minimum needed of technical specifications of information formats. In other words, standardization should consider first to work on a semantic, multi-language glossary, good practices for response planning and pan-European exercises/crisis debrief, organizational interoperability, the establishment of a command & control interoperability reference model, including areas for information to share, and resilience (understood here as agility and adaptability).

In a second phase standardization work should focus on more technical subjects to facilitate interoperability and improve the EU citizen experience: structure of geospatial information, warning systems (technical aspects to facilitate reception and common language to facilitate transmission and understanding), detection and reporting mechanisms using digital media, and first responders practical tools (communication systems, localisation of victims/affected people/responders, assistance to victims management), with a bottom-up approach.

It is only in a third phase that enablers for information systems interconnection and common information architecture for security would be candidate for standardization, i.e. standardization of re-usable digital objects, message formats, standardization of terms, and development of metadata to describe the situations and the risks. In the meantime experimentations will be needed to show what is possible and generate interest from the political authorities.

In the same time we recommend to develop three parallel roadmaps, to present the work in such a way to address more "political" issues:

- Strategic consideration and political acceptance by Member States (to stress the importance of senior official's involvement and MS political support).
- Functional and information needs (semantic, organizational interoperability model, good practices, information to share, before, during and after the crisis, human aspects and resilience).
- Technical enablers (detection, reporting and warning applications, libraries and language, first responders tools, structuring of geospatial information and communication interoperability).

3.3.5 Results and recommendations

The next table gives an overview of the results. As shown in the table there are only subjects with priority 1 and 2. The workshop in which this was debated did not select significant subjects with priority 3 or 4.

In this table there are a lot of project names. These are all projects which can be easily found on the FP7 website, http://cordis.europa.eu/home_en.html.

Proposal	Priority	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
1. Need for an understandable roadmap of existing and planned standards							
1.1 Understandable roadmap of existing standards and planned standards	1	TR		- Help public authorities to understand usage of standards. - Help standardization developers to provide useful standards	- Facilitate compatibility, consistency and product development	- Public authorities - Standards developers - Security operators - Industry	- It would provide a basic framework for future research programs
2. Need for semantic and organizational standardization							
2.1High level overall presentation of standardized management systems	1	TR		- Get major stakeholders and Public Authorities to understand the use of standards and apply them	- Obtain support from public authorities and major stakeholders to standardization process	- Public authorities - Operators - Security providers - Industry	- It would provide a basic framework for future research programs
2.2 Semantic interoperability	1	TR + CWA		- First needed step towards interoperability	- Will show usefulness of standards and provide first level of interoperability	- Public authorities - First responders - Operators - Security providers - Industry	- It would provide a basic framework for future research programs - SAVE-ME
2.3 Standardization of map objects (icons and terms) and geospatial based information	1	EN		- To allow inter-agency and cross-border geospatial understanding and cooperation	- To establish common shared geospatial basic information systems on which to develop specific information systems	- Public authorities - First responders - Operators - Security providers - Industry	- It will allow future development of geospatial based information systems.
2.4 Geospatial basic information system for underground facilities and indoor buildings	1	EN		- To facilitate indoors emergency response	- Allow development of underground/indoors geospatial information	- First responders - Operators - Industry	- Needed by DP projects - SECUR-ED

Proposal	Priority	Deliverabl e		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
2.5 Organizational model to facilitate interoperability of command and control (C&C) centres	1	TR + CWA		- Key proposal to facilitate coordination and cooperation between Member States - Will facilitate understanding of the organization missions, information needs and communication to the public	- Needed step before any emergency information system interoperability project can be implemented	- M.S. Policy and Crisis Management Officers - Public authorities - Private operators - Crisis management Information systems developers	- Impact on all projects related to crisis management and civil protection information systems - E-SPONDER - ACRIMAS - CRISMA - Learning 4 security (L4S)
3. Need for guidance in crisis response planning							
3.1Guidance for emergency response planning (risk based planning, information to share, methodologies for incident qualification, decision making under uncertainty…)	1	CWA + EN		- Facilitate coordination and cooperation by using similar planning methods	- Impact for crisis management directors - Facilitate cooperation and eventually development of information systems interoperability between M.S.	- M.S. Policy and Crisis Management Officers - Public authorities - Private operators	- Collation of existing work plus additional work needed
3.2 Debrief principles for pan-European exercises and cross-border crises	1	CWA + EN		- Facilitate efficiency, and development of good practices for cooperation and coordination between M.S.	- Will contribute to facilitate organizational interoperability between M.S.	- Public authorities	- Pandora
3.3 Standardize object models for simulation	2	CWA + EN		- Facilitate modelling and simulation tools for training	- Speed-up development work	- Information system developers - First responders	- All projects related to simulation - INDIGO - SAVE-ME - SICMA - CRISIs

Proposal	Priority	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
3.4 Common model for structural and functional aspects of facilities	2	CWA + EN		- Facilitate modelling and training tools efficiency	- Useful for model developers	- Rescue personnel - Service providers	- SAVE-ME
4. Need for guidance for resilience							
4.1 Standardize post incident resilience	1	CWA + EN		- Improve EU resilience	- Develop resilience through agility, adaptability and resilient fall-back mode	- Public authorities - First responders - Operators	- Complement to ISO 22301 - PEP
5. Need for developing improved reporting and mass warning systems							
5.1 Standardize reporting with mobile phones/tablets	1	EN		- Allows rapid transmission of "victim ticket" - Avoid saturation of calls and facilitate access to PSAP	- Develop distress beacon applications	- EU ordinary citizen	Collaboration with EENA - ISAR+
5.2 Standardize alert messages (including geo-localization)	1	EN		- Obtain understandable alert message in one's own language	- Encourage software developers work	- EU ordinary citizen	- Research needed - Opti-Alert
5.3 Develop a common language for warning	2	EN		- Provide useful alert and notification message to end users	- Redevelop alert libraries and communication protocol	- EU ordinary citizen	- More specific use of CAP protocol - Opti-Alert - Alert4All (A4A)
5.4 Use of social media (to be confirmed)	2	TR or CWA		- Improve the way to utilize social media to detect, prevent, protect, report and rescue.	- Develop tools to utilize social media and detect weak signals	- EU ordinary citizen - Public authorities - PSAP	- Some research needed - COSMIC - PEP

Proposal	Priority	Deliverabl e		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
6. to improve operational efficiency							
6.1 Next generation radio-communication interoperability	1	EN		- Transmit V/D/I to/from emergency First Responder	- Use of mass market technologies (LTE) with FR specific requirements (e.g. group communica - tions and proximity service)	- First Responders	- Activity already handled at 3GPP, TCCA, ETSI and the WRC (to get radio frequencies) - INFRA - E-SPONDER - SAVE-ME - HIT-GATE - GERYON
6.2 Geo-localization in buildings and underground	2	EN		- Facilitate FR interventions	- Develop applications to assist FR during interventions	- First responders	- INFRA - E-SPONDER - SAVE-ME
6.3 Interoperability of unmanned search and rescue equipment	2	EN		- Facilitate efficiency of cooperation between M.S.	- Improve interoperability in this sector	- First responders	- INFRA - E-SPONDER - SGL FOR USAR - ICARUS - DARIUS
6.4 Standardization of dynamic information	2	EN		- Efficiency of real time emergency advice to the general public (i.e. evacuation information)	- Applications to optimize response in real time - Software providers	- EU ordinary citizen - Rescue personnel	- SAVE-ME
6.5 Standardization of victims management	2	EN		- Efficiency of cross-border victims management (victims data, patient management, rapid triage)	- Emergency information systems for medical care during mass casualties	- Victims - Emergency medical responders	- Collation of good practices - FASTID - BOOSTER

Proposal	Priority	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		EN, TS, TR, CWA		Why is this an important proposal?	What will be the impact of the deliverable, especially for industry?	Who will use this deliverable, for what aim and how often will it be used?	What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?
7. Awareness							
7.1 Good practice for local territorial communities	2	CWA		- Efficiency and cooperation at the local level	- Development of specific information systems	- EU ordinary citizen - Local territorial communities	- PEP
7.2 Define common European message schemes	2	EN		- Citizen would better understand risks and adapt correct behaviour during emergency situation	- Develop alert libraries and information systems	- EU ordinary citizen	- Alert4All (A4A)
8. Communication interoperability for command and control (C&C) centres							
8.1 Standardization of event description and digital objects	2	CWA + EN		- This task is critical for information system interoperability, shared situation awareness and coordination. But it needs previous work on organizational interoperability, semantics understanding information needs and planning practices	- It will allow development of crisis management information systems that are interoperable and really implemented.	- C&C practitioners - All command chain - First responders	- Revisit ISO 22351/53 - Research needed - FP6 OASIS - CRISMA - SAVE-ME - CRISYS - IDIRA - BRIDGE

Table 6: Priority 1 & 2 Roadmap Projects – Determining Strategic Design of Crisis Management

A high level of a work programme is shown in the following figure:

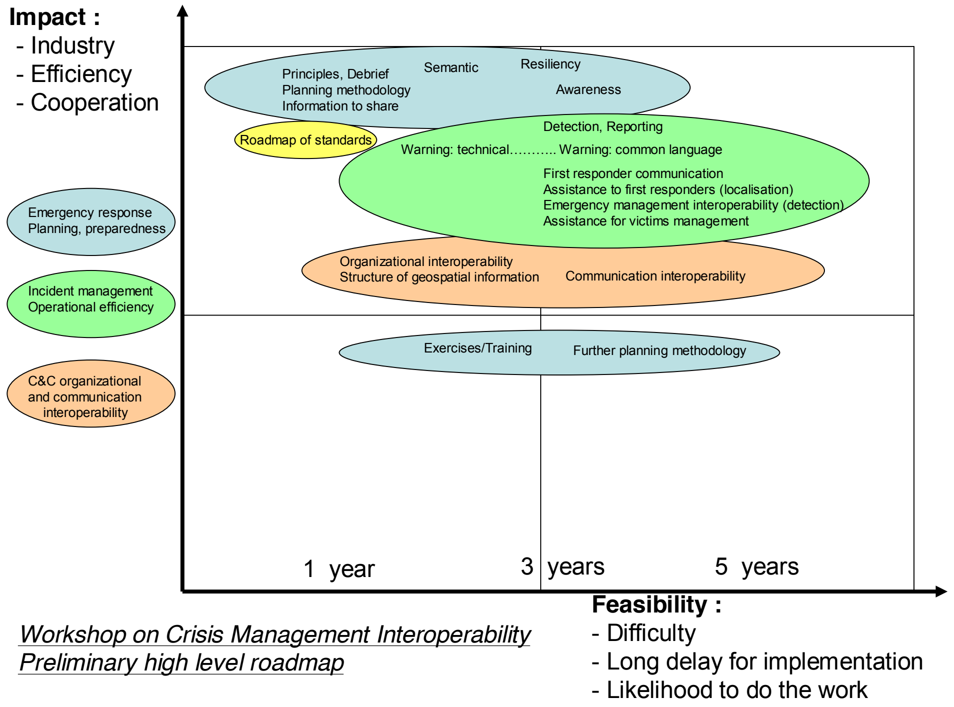

Impact :
- Industry
- Efficiency
- Cooperation
Emergency response
Planning, preparedness
Incident management
Operational efficiency
C&C organizational
and communication
interoperability
Principles, Debrief
Planning methodology
Information to share
Semantic
Resiliency
Awareness
Roadmap of standards
Detection, Reporting
Warning: technical.......... Warning: common language
First responder communication
Assistance to first responders (localisation)
Emergency management interoperability (detection)
Assistance for victims management
Organizational interoperability
Structure of geospatial information
Communication interoperability
Exercises/Training
Further planning methodology
1 year
3 years
5 years
Feasibility :
- Difficulty
- Long delay for implementation
- Likelihood to do the work
Workshop on Crisis Management Interoperability
Preliminary high level roadmap

Figure 6: High level work programme Crisis Management

In this figure, some items identified for further analysis or for good practices could easily be added, and would consolidate it.

Finally it is recommended to establish three parallel road maps:

1. One roadmap focusing on political acceptance and strategic issues. This is not a roadmaps of standards, but a roadmaps of political acceptance, through senior level meetings, demonstrations and political statements.
2. One roadmap focusing on functional aspects and formalisation of communication and interoperability needs and semantics.
3. One roadmap focusing on technical aspects of minimum requirements to respond to the needs with minimum constrains on public or private organizations (in term of costs, processes or organizational aspects).

These roadmaps could be the following ones:

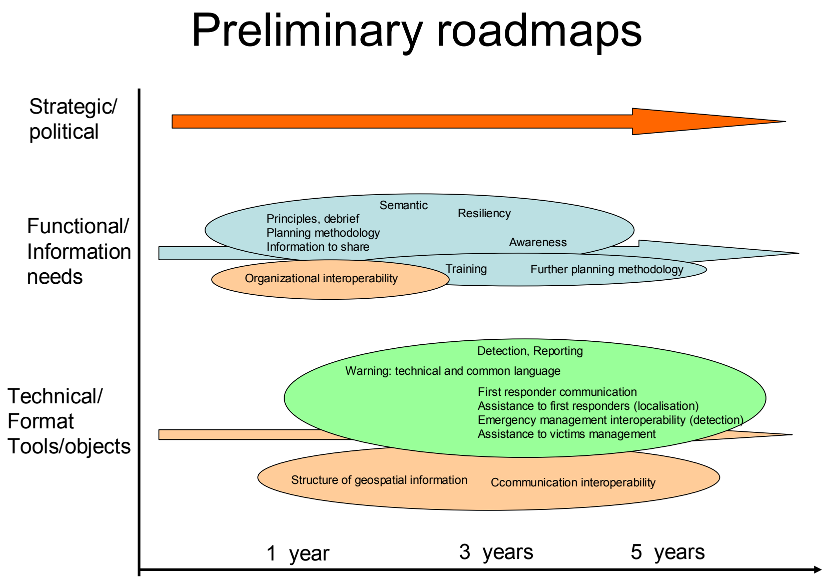

Preliminary roadmaps
Strategic/ political
Functional/ Information needs
Semantic
Principles, debrief
Planning methodology
Information to share
Resiliency
Awareness
Training
Further planning methodology
Organizational interoperability
Technical/ Format Tools/objects
Detection, Reporting
Warning: technical and common language
First responder communication
Assistance to first responders (localisation)
Emergency management interoperability (detection)
Assistance to victims management
Structure of geospatial information
Ccommunication interoperability
1 year
3 years
5 years

Figure 7: Roadmaps Crisis Management

Further recommendations

International standardization is carried out in the area of risk management, crisis management and business continuity, particularly in ISO/TC 223. Therefore, it is recommended that CEN/TC 391 works in close cooperation with ISO/TC 223.

In CEN/TC 391 agreements are made to handle the European adoption of the standards deliverables coming from ISO/TC 223. Depending on the results of different rounds of voting, some standards might be EN standards soon.

A lot of work has also been done and is still under development for FP6 and FP7 projects or CIPS projects. The results of these projects would usefully be mentioned on the proposed crisis management roadmaps presentation.

CEN/TC 391 will liaise with research projects that have been mentioned during the workshop and capitalization is needed; examples are the following ones; OASIS, E-SPONDER, INDIGO, INFRA, CRISYS, ISAR+, COSMIC, SAVE ME, ACRIMAS, CRISMA, PEPPOL, ISITEP. Other relevant projects that were not mentioned during the workshop are included in the above table 6. Most of them are within FP7 and one can find the objectives and other information of these projects on http://cordis.europa.eu/home_en.html.

A particular consideration should be given to experiments (i.e. Demonstration Projects) and to real implementation of technical inter-agency interconnections, such as the Netherlands pilot project that includes a common approach on information architecture for security.

The important consideration still remains: technical solutions should look at modest developments, responding for functional needs, with the minimum set of requirements to be accepted. There is a clear need to focus on some simple and practical solutions which can be trialled first, with the integration of the technical, processes and human aspects inherent to crisis management. CEN TC 391 can work on this and under the Vienna agreement co-operate with ISO/TC 223

3.4 Results of CBRNE

3.4.1 General

Broad consensus exists under the participants in this project that for most efforts aimed at an increase ‘impact’ and/or ‘defragmentation’ in the field of CBRNE to be effective, some degree of international ‘standardization’ will be required – both as a way to *regulate* (‘top-down’) as well as a way to *learn from others and to overcome resistance/roadblocks* (‘bottom-up’).

Insufficient (meta) information is currently available to link and provide an overview of various projects, programs, products, technology, market segments and ‘lessons learned’/residual knowledge on best practices - within and between the various stakeholder categories.

Aside from the specific priority actions (‘quick wins’) identified, a common and shared frame of reference needs to be developed which includes actions to be taken on items as diverse as ‘*semantics and terminology*’, ‘*system modeling*’ and ‘*cost-benefit analyses of (joint) resource and asset protection*’.

Standardization 'gaps' that have been identified are:

- Standards for Explosive Trace Detection equipment (ETD), used in Aviation Security (AVSEC).
- Standards for list-mode data acquisition based on digital electronics.
- Standards for Full Face Air Purifying Respirators (APR).
- Standards for Personal Protective Clothing (PPC) (including gloves and footwear) used to protect against Chemical, Biological, Radiological, and Nuclear (CBRN) Agents.
- Standard for “First Responder CBRE and low Oxygen level warning instrument” (“PWARN”) a FR (personal) detector including CBREO sub detectors to warn the FR in defined levels of contamination (mini).
- Standards for trace detection.
- The standards needed for reference materials for the missing CBRNE agents in various types of samples.
- Standard testing and evaluation (T&E) methodologies to assess the performance of CBRNE Sampling and Detection equipment.
- EU-wide explosive detection standards and testing methodologies for trace particle and vapour based threats.
- Standard(s) for sensors and sensor data**.**
- Common interoperability standards between CBRNE detection and sampling equipment and end-users, between networked devices and systems for CBRNE detection and sampling equipment for the capture, processing, communication of data, as well as the display and reporting of results to end-users and decision makers.

Recommendations:

- Establish a Community-of-Interest (COI) which:
  - brings all stakeholder categories together around the central theme of ‘CBRNE’;
  - functions as an independent entity under the guidance of national and international Standardization Organizations;
  - works in close coordination with CEN TC 391, WG 2 on CBRNE;

- Establish an inventory of projects, programs, products technology, market segments and 'lessons learned'/residual knowledge on best practices – within and between the various stakeholder categories.
- Even though the scope of this report is "*CBRNE – Chemical, Biological, Radiological, Nuclear and Explosives – with a focus on minimum detection standards as well as sampling standards, including in the area of aviation security*", it should be born in mind that this specific focus cannot effectively be dealt with when viewed in isolation from other, more over-arching security considerations such as:
  - The need for an 'all-hazard' approach (intentional, incidental, man-made or not, natural or technological, etc.);
  - The need to integrate and interconnect the various stages of an event including prevention (incl. deterrence), preparedness (early warning systems incl. sampling and detection), response, recovery and rehabilitation;
  - The need to link the economic impact of the (cascading) effects of a (partial) collapse of *critical infrastructure* (CI)[3] with the psychological impact of the (cascading) effects of a (partial) collapse of *societal and citizen's security*;
  - The need to quantify both the economic and societal impact-value-benefit of any priority actions identified in this and other reports – and linking the results with existing and planned research and technology development activity;
  - The realization that 'standardization' is a consensus-driven process and often requires specialized knowledge and expertise of SDO's: Standards Development Organizations.

3.4.2 Stakeholders and standardization landscape

Because of a cluttering of the many different standards amongst the many stakeholders in this field the overview of standards was linked to the different stakeholder categories. This is analysed and described in detail in Annex D.

A large number of stakeholders can be found for CBRNE:

Stakeholder categories
Manufacturers/suppliers in CBRN detection
Standards development organizations
Government/regulatory agencies
R&D/testing laboratories
Military
Producers/users
Citizens/population at large

Table 7: Stakeholder categories for CBRNE

3.4.3 Workshop

Prior to the workshop 70 proposals had been divided into four categories.

Each group reviewed and discussed all proposals to determine which ones are the most viable to take forward.

Categories	Key words
A Prevention	Sampling, detection, monitoring
B Response	First responders (FR) Public Safety

[3] Critical infrastructure: any public or privately owned system, service and physical network for which the disruption or destruction would have significant impacts on the functioning of society.

Categories	Key words
	Organisations (PSO), Public
C Consequence Management	Diagnosis/therapy, DSS, decontamination
D Consolidation	Reference materials, best practices, evaluation, lessons (not) learned, SOP's interoperability

Table 8: Categories workshop CBRNE

3.4.4 Standardization needs and gaps

In this field a number of sampling and detection standards have been developed for environmental reasons but they are not applicable for security.

Based on research, interviews and workshops it is concluded that:

1. The most persistent needs and gaps are related to the lack of the exchange of (meta) information to link and provide an overview of various projects, programs, products, technology, market segments and 'lessons learned'/residual knowledge on best practices - within and between the various stakeholder categories.
   Examples:
   - ITRAP+10 project (Illicit Trafficking Radiation Detection Assessment Programme, initiated by EC-DG JRC, inviting US-DHS and IAEA to participate), where about 100 detectors of different types used in border monitoring are tested according to procedures based on a common denominator of IEC, ANSI and IAEA standards and recommendations. ITRAP+10 project is implemented by the EC JRC institute for trans-uranium elements and the institute for reference materials and measurements. http://IRMM.jrc.ec.europa.eu and http://ITU.jrc.ec.europa.eu.
   - IEC/SC45B, WG15 (border monitoring) which developed several standards for testing border monitoring equipment for the detection of radioactive and nuclear material.
     http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1360,25
   - For proposals related to PPE, many standards are already there (e.g. OSHA), and the issue is on how to adopt them as European standard.
   - For proposals related to (handheld) detection of radio nuclear material: IEC 62618 and IEC 62401
   - The SLAM project (standardization of laboratory analytical methods, a FP7 Security Research Project, http://www.cbrnecenter.eu/project/slam/). On this subject information has been exchanged in a meeting in June this year in Stockholm.

2. Lack of commonly accepted definitions of CBRNE materials, methods, threats or incidents

3. Lack of general information on Standards Development Organizations (SDO's) and how the process of "standardization" actually works

4. The absence of EU-wide standards, testing and the certification of security equipment has been a major cause for the fragmentation of the European Security market which hampers investments, efficiency, and which slows down the EU's ability to respond and adapt quickly to new and emerging threats. This absence also

hinders interoperability as a major driver for the harmonization of the European Security market.

5. It is often unclear whether the detection standardization effort is directed at establishing minimum or critical levels of what needs to be measured or is directed at the device or technology that is used to measure. Without standards for detection levels of the equipment it is not possible to standardise hand-held equipment for the First Responders or to standardise test protocols for such equipment.

6. Many of the proposals are unclear and focus on ‘safety’ rather than ‘security’ – which points back to the lack of commonly accepted definitions, for instance ‘security’ defined as: "protection against threats by terrorism, organised crime, natural disasters, pandemics and major technical accidents".
   According to IAEA, the nuclear security is the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear or other radioactive substances or their associated facilities

7. Not all of the standardization of Testing & Evaluation has been worked on under ‘field’ conditions but mainly under laboratory conditions.

8. Many initiatives have been taken on both the civilian as well as military sides, but they largely represent industrial or sector standards delivering partial instead of integrated solutions.

9. The civilian side should more actively pursue an exchange with the military side. Not only because the claim is made that ‘NATO is leading in standards in the CBRNE domain’ but also because some doctrines are well established within the military whereas defragmentation is the rule on the civilian side.

10. In terms of Civil-Military Cooperation (CIMIC) standardization of decontamination/handover procedures and testing & evaluation of equipment can have impact – but not so much in terms of products but in terms of interoperability and standard operating procedures (SOPs).

11. The private sector companies and the end-users (civilian) are under-represented in the CBRNE sampling and detection standardization process.

12. The main challenge is to build a community of interest where all the different stakeholders are adequately represented. Without that, it will be difficult to fully estimate the needs and justify the on-going involvement by all stakeholders in standardization activities.

13. Quick wins with maximum impacts for competitiveness can only be achieved by the development of terminology standards and test methods and analysis standards for CBRNE detection technologies and devices. If the roadmaps are meant to be the backbone of a European standardization strategy in the CBRNE domain, that would constitute the fundamental layer to build from.

14. Member States will support the initiative of the Commission to develop the European security market when it mirrors the efforts conducted at the national levels both in terms of de-fragmentation of the security market and in terms of standardization activities.

15. The limitation of access by the manufactures to CBRN materials represents a real problem for testing and improving their production.

Summary of findings

Considerable and complex problems were encountered in aligning the differing public and private interests and strategies, the wide range of stakeholder categories involved, and the different thematic areas that fall within the acronym of ‘C-B-R-N-E’. The interviews conducted and the approximately 70 proposals received and reviewed in the workshop confirmed the central problem within the CBRNE (detection and sampling standards) domain as fragmentation.

At the same time, most CBRNE stakeholders categories at trans-national and national levels, be they Manufacturers and Suppliers, Standards Development Organizations, Governmental/Regulatory Agencies, R&D/Testing Laboratories, Military, Procurers and Users or Citizens/Population-at-large, including key players such as the EC and its JRC and EDA, NATO, UN, OPCW, WHO, IAEA, CEN-CENELEC, ISO, IEC, IEEE-AS, ASTM, ANSI, NIST, DIN, AFNOR, BSI, NEN, etc., are unified in their efforts to look for ways and means to increase impact.

Therefore it is recommended that in the evaluation process of future project proposals in the area of CBRNE their impact on bridging the gap between ‘fragmentation’ and ‘impact’ will be included.

Also suggestions are given from all participating entities – both in a general sense as well as in more specific terms – for further activity and present ‘roadmaps’ that can be used for short term progress (‘quick wins’) as well as facilitate middle and longer term benefits.

Of particular note was the observation that many of the workshop participants - representing CBRNE manufacturers, suppliers, procurers, users, government agencies and testing laboratories - seemed unfamiliar with some of the specific terms and the role of Standard Developing Organizations (SDO). For instance the term ‘standardization’ was taken by many to mean ‘standards’ instead of the standardization ‘process’ (which includes not only ‘standards’ *per se* but also other publications such as ‘technical specifications’, ‘guidelines’, ‘workshop agreements’, ‘best practices’ etc.).

3.4.5 Roadmaps

A high level of work program is shown in the following figure.

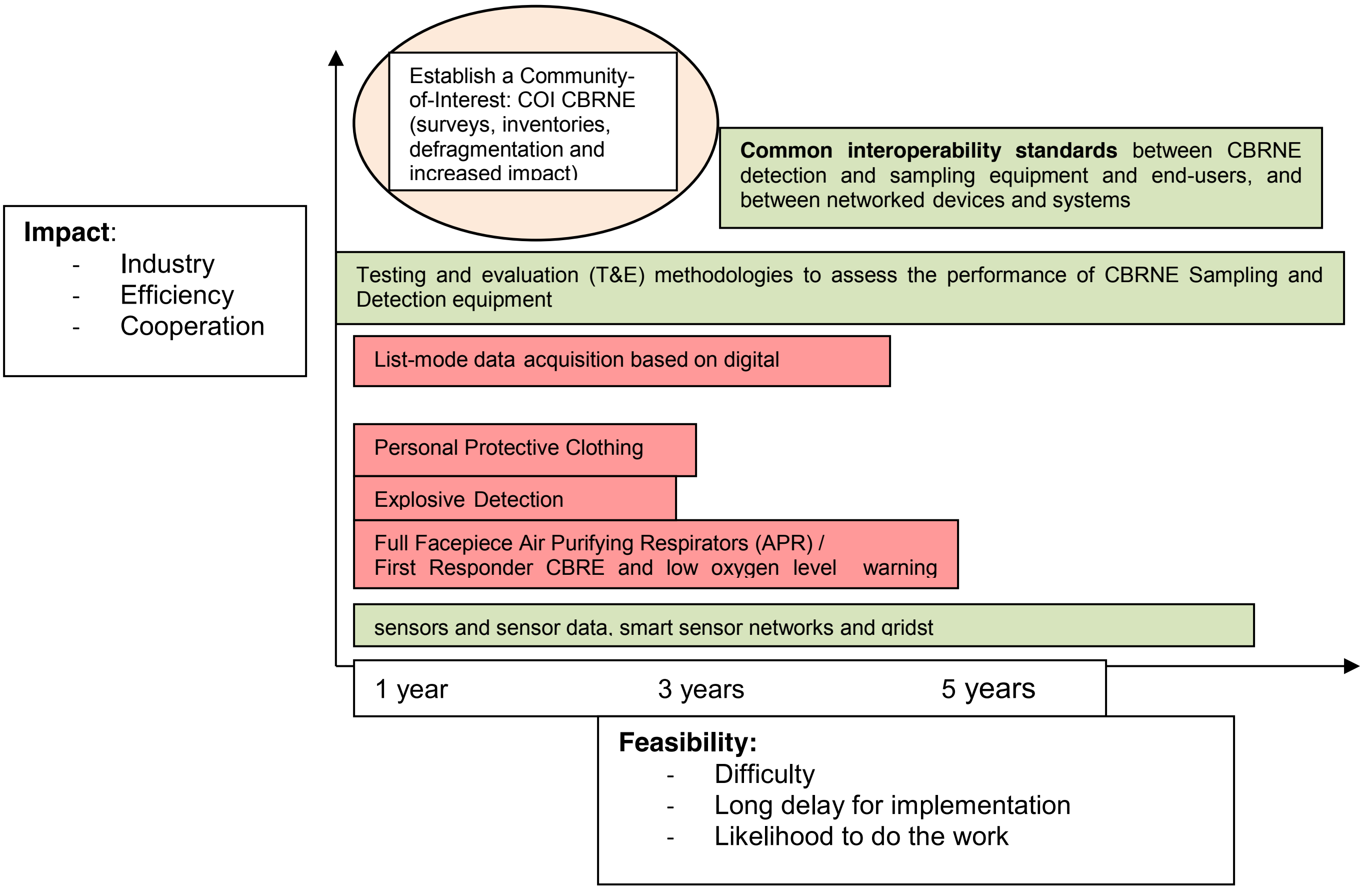

Establish a Community-of-Interest: COI CBRNE (surveys, inventories, defragmentation and increased impact)
Common interoperability standards between CBRNE detection and sampling equipment and end-users, and between networked devices and systems
Impact:
- Industry
- Efficiency
- Cooperation
Testing and evaluation (T&E) methodologies to assess the performance of CBRNE Sampling and Detection equipment
List-mode data acquisition based on digital
Personal Protective Clothing
Explosive Detection
Full Facepiece Air Purifying Respirators (APR) / First Responder CBRE and low oxygen level warning
sensors and sensor data, smart sensor networks and gridst
1 year
3 years
5 years
Feasibility:
- Difficulty
- Long delay for implementation
- Likelihood to do the work

Figure 8; High level work program CBRNE

The discussions in the workshops and the comments on the draft version of the report of phase 2 of Mandate M/487 have led to several results and recommendations as shown in table 9.

Proposal	Priority	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
EXPLOSIVES							
EXPLOSIVES To develop standards for Explosive Trace Detection equipment (ETD), used in Aviation Security (AVSEC) Plus: To develop Standard Test Piece (STP) for Liquids Explosive Detection Systems (LEDS) equipments	1			There are no minimum standards defined yet for ETD's in AVSEC field. There is no a such test piece for liquid explosives detection	It will serve to allow airports or the entities responsible of screening to make use of ETD equipment meeting the same minimum standards, which would otherwise be difficult in the absence of defining the performance requirements.	Industry, end-users, civil aviation authorities and entities involved in the AVSEC field	**PLEASE NOTE:** **A programme is already underway between DG ENTR, DG JRC and ECAC to develop an EU testing methodology for Aviation Security equipment.**
RADIATION							
RADIATION To develop standards for list-mode data acquisition based on digital electronics	1			Digitization and associated time-stamping of pulse trains from radiation detector systems enables more robust and "transparent" assay of radioactive samples. The data acquired in "list-mode" may be scrutinized by a variety of software algorithms, providing an unprecedented level of	Critical decisions made by responders to radiation contamination incidents may be scrutinized and confirmed by "off-site" experts, adding to the confidence in results via scrutiny of calculations, and improving	First responders to radiation contamination incidents, public safety organisations, border control, Industry, National Metrology Institutes, Radiation Protection Institutes.	I-TRAP+10, CATO

Proposal	Priority	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
				confidence in the results.	transparency of results. Increased safety and reduction of health risks to first responders, population and employees. Can avoid costly errors in incorrect designation of sites as contaminated with radioactivity. Creates many possibilities for industry.		
				Rising technology that will improve the sensitivity and the reliability of the measurement.	Time stamped list-mode data format produces significant added value compared to more conventional spectrum format. It improves source localization, allows signal-to-noise optimization, noise filtering, some new gamma- and neutron detectors even require list-mode to function. List-mode approach	Industry, defence forces, public safety organisations, police, border control, customs, fire fighters	

Proposal	Priority	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		EN, TS, TR, CWA		Why is this an important proposal?	What will be the impact of the deliverable, especially for industry?	Who will use this deliverable, for what aim and how often will it be used?	What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?
					also allows precise time synchronization of multiple detectors enabling, for example, simultaneous singles and coincidence spectrometry such as singles gamma and UV-gated gamma spectrometry.		
CBRN							
CBRN To develop standards for Full Facepiece Air Purifying Respirators (APR)	1			To provide respiratory protection from CBRN agent's inhalation hazards	Increased safety and reduction of health risks to first responders, population and employees. Correlation with Personal Protective Equipment (PPE) of first responders. Creates many possibilities for the industry	Industry, First responders, public safety organisations	IF REACT, ARCHIMEDES
CBRN To develop standards for Personal Protective Clothing	1			To protect the skin from various CBRN health hazards that may be encountered in the workplace	Increased safety and reduction of health risks to first responders,	Industry, First responders, public safety organisations	IF REACT, ARCHIMEDES

Proposal	Priority	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
(PPC) (including gloves and footwear) used to Protect Against from Chemical, Biological, Radiological, and Nuclear (CBRN) Agents				or during a terrorist attack	population and employees. Correlation with Personal Protective Equipment (PPE) of first responders. Creates many possibilities for the industry		
CBRN To develop standard testing and evaluation (T&E) methodologies to assess the performance of CBRNE Sampling and Detection equipment	1/2			To provide common test-methods, accredited test facilities, and reference materials containing uniform guidance to government, industry and first responders on the capabilities and limitations of available CBRNE Sampling and Detection equipment.	Increased safety and reduction of health risks to first responders, population and employees	Industry, First responders, public safety organisations	SLAM, CATO, ARCHIMEDES, PRACTICE, EQUATOX
To develop common interoperability standards between CBRNE detection and sampling equipment and end-users, and between networked devices and systems for CBRNE detection and sampling equipment for the capture, processing, and	2			Improve response to a CBRNE incident , lowers the cost and contributes to uniform implementation by responders	Increased safety and reduction of health risks to first responders, population and employees.	Industry, public safety organisations, government, industries at risk, first responders, public	SLAM, PRACTICE, CATO, IF REACT, ARCHIMEDES, EQUATOX

Proposal	Priority	Deliverable		Importance	Impact	Users	Relationship other projects
What is the exact proposal?		**EN, TS, TR, CWA**		**Why is this an important proposal?**	**What will be the impact of the deliverable, especially for industry?**	**Who will use this deliverable, for what aim and how often will it be used?**	**What is the relationship with research projects (FP7 / Horizon 2020 / etc.)?**
communication of data, as well as the display and reporting of results to end-users and decision makers.							
Standard(s) for sensors and sensor data The idea is that new sensors will become more like computer components; and because they conform to standards they can therefore easier, faster and cheaper being integrated in operational sensor units or systems.	2			Easier and faster time to market of new sensor developments. - Sensor developers can focus on new sensors. - They do not have to design and produce of; and develop software for the sensor unit or system. - No problem with entering the end-user market with a new brand and/or product. - Vendors of sensor units and systems who already have a market presence can more easily, quickly and cheaply integrate new sensor developments in new and existing sensor units, systems, products or services.	Easier, faster and cheaper operational availability of new sensor applications. Less separate (or dedicated) units or systems with each having its own user interface, way of handling and maintenance.	sensor developers , vendors of sensor units and systems, system integrators, CBRNE experts, (public and private) safety and security bodies and companies	CATO, SLAM, IF REACT, INNOSEC, PRACTICE, EQUATOX

Table 9: Priority 1 & 2 Roadmap Projects – Determining Strategic Design of CBRNE

GENERAL

- Broad consensus exists under the participants in this project that for most efforts aimed at an increase in 'impact' and/or 'defragmentation' in the field of CBRNE to be effective, some degree of international 'standardization' will be required – both as a way to *regulate* ('top-down') as well as a way to *learn from others and to overcome resistance/roadblocks* ('bottom-up').
- Insufficient (meta) information is currently available to link and provide an overview of various projects, programs, products, technology, market segments and 'lessons learned'/residual knowledge on best practices - within and between the various stakeholder categories.
- Aside from the specific priority actions ('quick wins') identified, a common and shared frame of reference needs to be developed which includes action to be taken on items as diverse as '*semantics and terminology*', '*system modeling*' and '*cost-benefit analyses of (joint) resource and asset protection*'.

SPECIFIC

- Four proposals received a unanimous score of 1 ('quick wins') by at least 4 of the 6 groups.
- There were some proposals classified as Priority 1 + 2 by at least 4 of the 6 groups and were therefore slated for further review and commentary.

Further recommendations

- Establish a Community-of-Interest (COI) which:
  - brings all stakeholder categories together around the central theme of 'CBRNE'
  - functions as an independent entity under the guidance of national and international SDO's
  - works in close coordination with CEN TC 391, WG 2 on CBRNE.
- Establish an inventory of projects, programs, products technology, market segments and 'lessons learned'/residual knowledge on best practices – within and between the various stakeholder categories.
- Even though the scope of this report is "*CBRNE – Chemical, Biological, Radiological, Nuclear and Explosives – with a focus on minimum detection standards as well as sampling standards, including in the area of aviation security*", it should be born in mind that this specific focus cannot effectively be dealt with when viewed in isolation from other, more over-arching security considerations such as:
  - the need for an 'all-hazard' approach (intentional, incidental, man-made or not, natural or technological, etc.);
  - the need to integrate and interconnect the various stages of an incident including prevention (incl. deterrence), preparedness (early warning systems incl. sampling and detection), response, recovery and rehabilitation;
  - the need to link the economic impact of the (cascading) effects of a (partial) collapse of *critical infrastructure* (CI) with the psychological impact of the (cascading) effects of a (partial) collapse of *societal and citizen's security*;
  - the need to quantify both the economic and societal impact-value-benefit of any priority actions identified in this and other reports – and linking the results with existing and planned research and technology development activity;
  - the realization that 'standardization' is a consensus-driven process and often requires specialized knowledge and expertise of SDO's: Standards Development Organizations.

4 Follow up and introduction to the annexes

4.1 Follow-up

To share the results of this report with stakeholders and to get feedback on how to continue the work done, a number of proposed activities in the near future is given for each of the three sectors.

As far as the European Commission is concerned, with the submission of this M/487 Phase 2 report to the Commission the recommendations of CEN/TC 391, based on the interactions with stakeholders during Phase 2, for initiating concrete standardisation actions in the three investigated areas – border security, crisis management/civil protection and CBRNE, are tabled. In a next step, starting end of 2013, the Commission can draft Standardisation Mandates for these three areas, outlining concrete standardisation needs, based on the recommendations of this report.

CEN TC 391 will discuss the outcomes of this Phase 2 of M/487 in its meeting October 2 and 3, 2013 in Paris, and with the liaisons of CEN TC 391, to support the EC in its decisions.

Proposed follow-up activities for ABC

As well as pursuing standardisation as stated above, there is scope for activity within the European border agency community and technology industry in particular for “awareness sessions” on:

- Commonality of technical standards for the components so that operators know exactly what they are purchasing and how it will perform;
- Commonality of the ‘look and feel’ of ABC systems so that passengers intuitively know how to use different systems;
- Commonality of standards for the operators’ interface so that border agency staff are protected from stress and physical strain.

These subjects can most easily be promoted via subject trade shows and conferences such as the Frontex Global ABC Conference (October 2013, Warsaw) Biometrics 2013 (October 2013, London), Workshop on Innovation in Border Control (August 2013, Uppsala) Security Document World (May 2014, London), ID World (November 2013, Frankfurt), Borderpol Congress (December 2013, London).

Proposed follow up activities for crisis management

Referring to the fact that one of the findings of this Phase 2 was that the knowledge and awareness of the benefits of standardisation in the crisis management community is rather little, it is suggested to particularly address this need through dedicated workshops and conferences, e.g. with high-level attendance, to foster the relationships between the crisis management and the standardisation community.

One example of such an event could be the upcoming Milipol Exhibition and Conference on internal state security in Paris (19 – 20 November 2013).

Proposed follow-up activities for CBRNE

As discussed in the chapter on CBRNE, the stakeholders of CBRNE - such as EC DG JRC, the European Defence Agency, producers, end users - will form communities of interest (COI) where results of workshops and seminars will be shared to optimize the work and to align with research programmes. Such a COI should include in particular the European Defence Agency (EDA) with its defence stakeholders dealing e.g. with tests and evaluation of CBRNE detection equipment.

4.2 Description of the annexes

Lots of information has been gathered throughout this research. Not all has been added to the main text in order to keep it readable.

In **Annex A** a list of abbreviations has been added.

For each of the priority sectors a separate Annex has been developed.
Annex B for Border Security;
Annex C for Crisis Management/Civil protection;
Annex D for CBRNE.

In each of these annexes there is an overview of existing standards and the results of the workshops.

5 Bibliography

[1] Security Industrial Policy Action Plan for an innovative and competitive Security Industry
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0233:FIN:EN:PDF

[2] Mandate M/487 to Establish Security Standards - Final Report Phase 1 - Analysis of the Current Security Landscape
ftp://ftp.cen.eu/CEN/Sectors/List/SecurityandDefence/SecurityoftheCitizen/M487Phase1_report.pdf

[3] A strategic vision for European standards: Moving forward to enhance and accelerate the sustainable growth of the European economy by 2020
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0311:FIN:EN:PDF

[4] ICAO:
Guidelines – Electronic Machine-readable Travel Documents &Passenger Facilitation version 1.0, April 17 2008

[5] Frontex:
Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, Research and Development Unit 31/08/2012 Version 2.0

[6] Frontex:
Best Practice Operational Guidelines for Automated Border Control (ABC) Systems, Research and Development Unit 31/08/2012 Version 2.0

[7] European Commission
Regulation 2252/2004 and 810/2009 of the European Union

CEN/TS 16634	Recommendations for using biometrics in European automated border crossing.
ISO 22300	Societal security - Terminology, 2012
ISO 22301	Societal security — Business continuity management systems — Requirements
ISO/DIS 22324	Social Security – Emergency Management
ISO/FDIS 22398	Societal security -- Guidelines for exercises
ISO 31000	Risk management — Principles and Guidelines 2009
ISO/DTR 22351	Societal security -- Emergency management -- Message structure for exchange of information
IEC 62618	Radiation protection instrumentation – Spectroscopy-based alarming Personal Radiation Detectors (SPRD) for the detection of illicit trafficking of radioactive Material, 2013
IEC 62401	Radiation protection instrumentation – Alarming personal radiation devices (PRD) for detection of illicit trafficking of radioactive material, 2007
ISO/DIS 22322	Societal security -- Emergency management -- Public warning
ICAO 9303	Machine Readable Travel Documents, part 1-3,

Annex A
(Informative)

List of abbreviations

Organizations:

ABC	Automated Border Control
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
EC	European Commission
EENA	European Emergency Number Association
EOS	European Organization for Security
EU	European Union
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
3GPP	3rd Generation Partnership Protocol (collaboration between groups of telecommunications associations to develop mobile phone specifications)
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JRC	Joint Research Centre of the European Commission
MS	Member States
NEN	Netherlands Standardization Organization
NGO	Non-Governmental Organization
NSB	National Standardization Body
SDO	Standards Development Organizations
TCCA	TETRA + Critical Communications Association (association for the development of public safety and critical communications networks)

Others:

AVSEC	Aviation Security
APR	Air Purifying Respirators
CAP	Common Alerting Protocol
C&C	Command and Control
CI	Critical Infrastructure
COI	Community of Interest
CWA	CEN Workshop Agreement
EFFISEC	Efficient Integrated Security Checkpoints
ERNCIP	European Reference Network for Critical Infrastructure Protection
ETD	Explosive Trace detection
FP7	Seventh Framework Programme for Research and Technological Development form the European Commission
FR	First Responders
Horizon 2020	The EU Framework Programme for Research and Innovation
ITRAP	Illicit Trafficking Radiation Detection Assessment Programme
LTE	Long Term Evolution (high speed data mobile transmission)
MRTD	Machine Readable Travel document
PSAP	Public Safety Answering Point
PPE	Personal Protective Equipment
TC	Technical Committee

T&E	Testing and Evaluation
TR	Technical Report
TS	Technical Specification
TSO	Tactical Situation Objects

Annex B
(Informative)

Border Security

B.1 Existing standards

Existing Standards and Recommended Practices within Those Components

- Passengers

Fortunately, the species *homo sapiens* generally starts out with standard design, though it may vary in colour and size and environmental conditions may degrade the "specification" over time. The vast majority of people who travel internationally, and thereby become candidates for ABC use, possess the necessary biometric features which can be captured and matched by ABC systems. A normal but unique facial configuration with eyes, nose and mouth in roughly the natural shape and/or fingers and thumbs with unique skin patterns and/or two eyes with uniquely patterned irises are all that are required. Clearly passengers must have sufficient mental and physical capability to negotiate ABC systems and those which lack any of the aforementioned features or capabilities will need to be handled by alternative means.

Human beings do not have 'standards' as such but see the *Eligibility Rules* and *User Familiarisation* sections below.

Document	Description
ISO/IEC WD TR 29194	Guide on designing accessible and inclusive biometric systems
ISO/IEC TR 19765:2007	Survey of icons and symbols […] to improve the use of IT products by the elderly and persons with disabilities
ISO/IEC AWI TR 30110	Biometrics and children
ISOIEC PDTR 29195	Technical Report on traveller processes for biometric recognition in automated border control systems
ISO 24501:2010	Specifies methods for determining the sound pressure level range of auditory signals so that the users of consumer products, including people with age-related hearing loss, can hear the signal properly in the presence of interfering sounds. Auditory signals, in ISO 24501:2010, refer to sounds with a fixed frequency (also called beep sounds) and do not include variable frequency sounds, melodic sounds, or voice guides. ISO 24501:2010 is applicable to auditory signals which are heard at an approximate maximum distance of 4 m from the product, as long as no physical barrier exists between the product and the user. It is not applicable to auditory signals heard through a head receiver or earphones, or to those heard with the ear located very near to the sound source because of the interference of the head with sound propagation. ISO 24501:2010 does not specify the sound pressure level of auditory signals regulated by other statutes, such as those for fire alarms, gas leakages and crime prevention, nor does it specify auditory signals particular to a communication tool such as telephones. ISO 24501:2010 does not specify auditory danger signals for public or work areas which are covered in ISO 7731, ISO 8201, and ISO 11429.

- Supervising border agency staff

Clearly the officers supervising ABC systems (there are very few unsupervised systems) need training to use the equipment effectively (for example, knowing how to react to events and alerts correctly) and historically the procedures have been compiled by the border agency in association with the system providers.

The UK however has been running 3 concurrent varieties of passport-activated ABC, each from a different phase or supplier but with a common user interface.

Also, there is no standard accepted number of ABC lanes that an individual officer might monitor at the same time. It was optimistically considered to be 5 or 6 lanes when systems were first introduced (Frontex guide?) but experience may have proved this to be an unreasonable demand on an officer's attention capability.

The standards which do apply here EU Directive on ICT Display Screens, which should have been absorbed in EU members states' national legislation (e.g. UK's display screen regs).

These are however for border agencies to satisfy in order to meet their nation health & safety legislation and possible diversity policies (e.g. use by disabled officers).

Document	Description
ISO/IEC 9241-171:2008	Ergonomics of human-system interaction – Part 171 Guidance on software accessibility
ETSI ES 202 432:(2006-05)	Human factors; Access symbols for use with video content and ICT devices.
ISO/IEC 24714-1:2008	Information technology – Biometrics – Jurisdictional and societal considerations for commercial applications – Part 1: General guidance
CEN CWA 14661:2003	Guidelines to Standardisers of ICT products and Services in the CEN ICT domain (accessibility)
ISO 9241-400:2006	Gives guidelines for physical input devices for interactive systems. It provides guidance based on ergonomic factors for the following input devices: keyboards, mice, pucks, joysticks, trackballs, trackpads, tablets and overlays, touch sensitive screens, styli, light pens, voice controlled devices, and gesture controlled devices. It defines and formulates ergonomic principles valid for the design and use of input devices. These principles are to be used to generate recommendations for the design of products and for their use. It also defines relevant terms for the entire 400 series of ISO 9241. For some applications, e.g. in areas where safety is the major concern, other additional principles may apply and take precedence over the guidance given here. ISO 9241-400:2006 also determines properties of input devices relevant for usability including functional, electrical, mechanical, maintainability and safety related properties. Additionally included are aspects of interdependency with the use environment and software.

- Operational and fall-back procedures

Obviously each border agency defines its own procedures for the use and monitoring of ABC systems but ICAO and Frontex have both published guidance containing recommended practices.

ISO 30125 technical report on the use of mobile biometrics for personalisation and authentication

Document	Description
ISO 29156	Guidance on security and usability

- Eligibility rules

The eligibility to pass through ABC lanes is generally limited to those passengers who have been previously enrolled or pre-cleared, or to those whose eligibility is based upon nationality and age. There may also be other tests, such as passport expiry date, enrolment expiry date and matches with passport or biographic watchlists.

Document	Description
ISO 30110	Technical Report which deals with biometrics and children
ISO 29144	The use of biometric technology in commercial identity management applications and processes
ISO 29196	Guidance for biometric enrolment

- User familiarisation

Passengers, crew and port staff generally require some kind of familiarisation instruction since large numbers of these will be using the ABC system for the first time or after a lengthy period. In these circumstances, guidance in the form of signage, video or audio instructions and human assistance is necessary. Since there will always be a supply of novice users, guidance must be assumed to be a standard feature of ABC. Each ABC system has its own level of detail and manner of presentation, even down to icons and text. There is no standard international guidance material but a set of icons has been published recently by ISO (24779) and a standard vocabulary for biometrics is in preparation. Text fonts are already standardised but the choice of font is not specified anywhere.

Document	Description
ISO 24779	Pictograms, icons and symbols for use with biometric systems
ISO 29144	Use of biometric technology in commercial identity management
ISO 29194	Guidance on Inclusive Design and Operation of Biometric Systems

- Travel documents and tokens

Travel documents (passports and ID cards used for travel) are almost all subject to ICAO's standards document ICAO 9303. Almost all issuing authorities have signed up to produce ICAO standard travel documents and probably all European passports will be fully compatible to ABC systems by 2016. ICAO9303 specifies the use of standards created by ISO/IEC JTC/1 SC37. ABC systems are designed to accept ICAO9303 documents and will general reject non-compliant items.

The modern version of the Seaman's Book (an identification document for merchant navy crew) is a standard document issued under the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185) of the International Labour Organisation and it contains fingerprint data which complies with ISO/IEC 19794 part 2.

Document	Description
ISO 7816-11:2004	Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods
ICAO 9303	Machine Readable Travel Documents INCITS/ISO/IEC 7501-1-1997
ISO 24787	On-card matching
ISO/IEC 19762-3:2005	Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part 3: Radio frequency identification (RFID)

Document	Description
	ISO/IEC 19762-3:2005 provides terms and definitions unique to radio frequency identification (RFID) in the field of automatic identification and data capture techniques. This glossary of terms enables the communication between nonspecialist users and specialists in RFID through a common understanding of basic and advanced concepts. Operator training: non-specialist users and specialists in RFID have a common glossary for terms related to the automatic identification and data capture techniques
CWA 15264:2005	Architecture for a European interoperable eID system within a smart card infrastructure
CWA 15535:2006	Smart Card Systems: Interoperable Citizen Services: Extended User Related Information
CWA 13987:2003	Smart Card Systems: Interoperable Citizen Services: Extended User Related Information

- Travel document data capture devices

There are no standards for document scanners or readers but all machine readable travel documents (MRTDs) and electronic machine readable travel documents (e-MRTD) should be read by such devices.

- Biometric capture devices

Document	Description
ISO 14443	RFID ISO/IEC 14443-2:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface
	OCR B Machine Readable Font

- Biometric matching techniques

Document	Description
ISO 30107	Anti-spoofing and liveness detection techniques

- Barrier mechanisms and sensors

Document	Description
IEC 60839	Alarm systems *n/a* Data exchange, harmonisation of functionality
EN 60950-1	Safety for information technology equipment *General requirements* Technological arrangements for the body electrical safety.

- System logic

- Biometric standards, data interfaces and security

Document	Description
ISO 19785	Common Biometric Exchange Formats Framework [CBEFF] –Standardised biometric information records. ISO/IEC 19785-1:2006
ISO 19784	Biometric Application Programming Interface [BioAPI]

Document	Description
ISO/IEC 24708:2008	Specifies the syntax, semantics, and encodings of a set of messages (BIP messages) that enable a BioAPI-conforming application (see ISO/IEC 19784-1) to request biometric operations in BioAPI-conforming biometric service providers (BSPs) across node or process boundaries, and to be notified of events originating in those remote BSPs. It also specifies extensions to the architecture and behaviour of the BioAPI framework (specified in ISO/IEC 19784-1) that supports the creation, processing, sending and reception of BIP messages. It is applicable to all distributed applications of BioAPI
ISO 24709	BioAPI Conformance
ISO/IEC 19794	Biometric Data Interchange Formats – Parts 2,4,5,6
ISO 19795	Biometric performance testing and reporting
ISO 24713	Biometric Profiles for Interoperability and Data Interchange 24713-1 Reference architecture 24713-2 Physical access control for airport employees 24713-3 Biometric identification and verification of seafarers
ISO 29156	Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
ISO 29109	Conformance testing methodology for biometric records
ISO 29794	Biometric sample quality
ISO 29197	Evaluation methodology for environmental influence in biometric system performance
ITU X.1142	eXtensible Access Control Markup Language (XACML 2.0) *n/a* Interoperable access control systems
29141	Ten fingerprint capture using BioAPI
ISO/IEC TR 24722:2007	Provides a description of and analysis of current practice on multimodal and other multibiometric fusion, including (as appropriate) reference to a more detailed description. It also discusses the need for, and possible routes to, standardization to support multibiometric systems.
ISO/IEC 29141:2009	Specifies requirements for the use of ISO/IEC 19784-1, as amended by ISO/IEC 19784-1/Amd.1 (BioAPI) for the purpose of performing a tenprint capture operation. It specifies a biometric data block format that is used to interact with a BioAPI framework [and hence with biometric service providers (BSPs)] to support an application wishing to perform a tenprint capture. It specifies a capture control block and a capture output block that conforming BSPs are required to support if they conform to ISO/IEC 29141:2009.
ISO/IEC 19792:2009	Specifies the subjects to be addressed during a security evaluation of a biometric system. It covers the biometric-specific aspects and principles to be considered during the security evaluation of a biometric system. It does not address the non-biometric aspects which might form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels). ISO/IEC 19792:2009 does not aim to define any concrete methodology for the security evaluation of biometric systems but instead focuses on the principal requirements. As such, the requirements in ISO/IEC 19792:2009 are independent of any evaluation or certification scheme and will need to be incorporated into and adapted before being used in the context of a concrete scheme. ISO/IEC 19792:2009 defines various areas that are important to be considered during a security evaluation of a biometric system. ISO/IEC 19792:2009 is relevant to both evaluator and developer communities:

Document	Description
	• It specifies requirements for evaluators and provides guidance on performing a security evaluation of a biometric system. • It serves to inform developers of the requirements for biometric security evaluations to help them prepare for security evaluations. Although ISO/IEC 19792:2009 is independent of any specific evaluation scheme it could serve as a framework for the development of concrete evaluation and testing methodologies to integrate the requirements for biometric evaluations into existing evaluation and certification schemes.

- E-Gate and kiosk construction

Document	Description
ISO 12543-1:2011	ISO 12543-1:2011 defines terms and describes component parts for laminated glass and laminated safety glass for use in building.
ISO 13849-1:2006	Provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. For these parts of SRP/CS, it specifies characteristics that include the performance level required for carrying out safety functions. It applies to SRP/CS, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery. It does not specify the safety functions or performance levels that are to be used in a particular case. ISO 13849-1:2006 provides specific requirements for SRP/CS using programmable electronic system(s). It does not give specific requirements for the design of products which are parts of SRP/CS. Nevertheless, the principles given, such as categories or performance levels, can be used.
ISO/TS 29584 :2012 ED1	Glass in building. Pendulum impact testing and classification of safety glass for use in buildings
BS 3193:1993	Thermally toughened glass panels for use where such panels can be exposed to thermal and/or physical shock. Methods of test for fragmentation and for resistance to thermal shock and impact, and recommendations to manufacturers on use.
BS 5357:2007	Code of practice for installation and application of security glazing
BS 6180 2011	Gives the latest recommendations and guidance for the construction of barriers in and around buildings. The standard applies to temporary and permanent barriers designed to protect people from hazards, restrict access or control vehicle traffic. BS 6180 outlines requirements for protective, crash and crush barriers as well as those that impose a speed limit of up to 16km/h (4.44m/s or 10miles/h). The standard does not apply to areas or buildings designed for spectator sports, construction sites or barriers to protect children younger than 24 months

- Business case, societal issues and system design methodology (PAS92)

Document	Description
ISO 30124	Code of practice for the implementation of a biometric system
ISO/IEC TR 24714-1:2008	Gives guidelines for the stages in the life cycle of a system's biometric and associated elements. This covers the following: • the capture and design of initial requirements, including legal frameworks; • development and deployment;

Document	Description
	• operations, including enrolment and subsequent usage; • interrelationships with other systems; • related data storage and security of data; • data updates and maintenance; • training and awareness; • system evaluation and audit; • controlled system expiration. The areas addressed are limited to the design and implementation of biometric technologies with respect to the following: • legal and societal constraints on the use of biometric data; • accessibility for the widest population; • health and safety, addressing the concerns of users regarding direct potential hazards as well as the possibility of the misuse of inferred data from biometric information. The intended audiences for ISO/IEC TR 24714-1:2008 are planners, implementers and system operators of biometric systems.
ISO/IEC 2382-37:2012	Harmonised biometric vocabulary
ISO/IEC TR 24741:2007	Describes the main biometric technologies, with some historical information. An annex describes the work of creating International Standards for biometrics and provides a layered model for the placement of the various International Standards being produced, with a short description of each. A second annex contains some of the terms and definitions currently used in these International Standards or the drafts of these International Standards.
ISO 24722	Multimodal Fusion
ISO 19092-1	Biometric security framework (TC68)
ISO/IEC 24761:2009	Specifies the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. ISO/IEC 24761:2009 allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrolment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion. ISO/IEC 24761:2009 specifies the cryptographic syntax of an ACBio instance. The cryptographic syntax of an ACBio instance is based on an abstract Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using either a compact binary encoding or a human-readable XML encoding. ISO/IEC 24761:2009 does not define protocols to be used between entities such as biometric processing units, claimant, and validator. Its concern is entirely with the content and encoding of the ACBio instances for the various processing activities.
ISO 19792	Security evaluation of biometrics
ISO/IEC 24745:2011	Biometric information protection
ISO/IEC 29164	Embedded BioAPI
ISO/IEC 19784	BioAPI security & sensor interface ISO/IEC 19784-1:2006
ISO/IEC 30106	Object Oriented BioAPI
ISO/IEC 30108	Biometric Identity Assurance Services (BIAS)
CWA 15499:2006	Personal Data Protection Audit Framework (EU Directive EC 95/46)
CWA 15263:2005	Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization

Document	Description
CWA 16113:2010	Personal Data Protection Good Practices
ISO 14915-2:2003	Provides recommendations and requirements for the design of multimedia user interfaces with respect to the following aspects: design of the organization of the content, navigation and media-control issues. ISO 14915-2:2003 is limited to the design of the organization of the content and does not deal with the design of the content in general. Design issues within a single medium (e.g. the lighting of a film sequence) are only addressed with respect to the ergonomic issues related to user controls.

B.2 Workshop

Program workshop at Warsaw

Workshop Agenda 4. April 2013		
13:00 – 13:30	Welcome and Introduction	Joost Cornet, Chair of M/487 coordination group Erik Berglund, Head of the Capabilities Division, Frontex Hans-Martin Pastuszka, EC DG Enterprise and Industry
13:30 – 14:00	Setting the Scene	Chris Hurrey, M/487 project expert for Border Security
14:00 – 15:30	Workshops: Areas A&B	All Participants
15:30 – 16:00	Coffee Break	All Participants
16:00 – 16:30	Workshops Continued	All Participants
16:30 – 17:50	Presentations: Areas A&B	Moderators
17:50 – 18:00	Closure	Joost Cornet
Evening	Evening Activity	Dinner
5. April 2013		
09:00 – 10:30	Workshops : Areas C&D	All Participants
10:30 – 11:00	Coffee Break	All Participants
11:00 – 11:30	Workshops Continued	All Participants
11:30 – 12:50	Presentations: Areas C&D	Moderators
12:50 – 13:20	Questions &Answers	Q&A for the coordination group M/487
13:20 – 13:30	Closure	Joost Cornet
13.30		Lunch

In the following tables a detailed description of the results of the workshop on Border Security is included. Each proposal is shaded. After each Proposal number there is a description of the proposal.

In the row below each proposal the outcome of the discussion during the workshop is included (including the choice of the priority, which is shaded).

After the workshop participants had the opportunity to comment on the proposals. The texts of these comments are shaded, preceded by the name of the commentator

A Technical standards

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
A1	Security of the passenger: Door resistance, automatic opening when obstructed.	Non-harmful to the passenger. What is the maximum pressure allowed when closing doors?	A combination of suppliers and border agencies/end-users, plus independent academics	Suppliers and purchasers	To avoid injury claim from passenger.
	TECHNICAL STANDARDS AREA: Safety design in automated barrier systems RECOMMENDED PROCEDURE AREA: **PRIORITY: 1** The group questioned the value of this, as there should already be something in place. Comment that in Europe, there have been quite some implementations of ABC, so makes more sense to make references to existing standards and safety requirements rather than to re- invent the wheel. Priority depends on whether such a standard already exist. If this standard exists, then just make reference to it. Implementation should then be fast and simple. If this standard does not exist, need to develop this standard.				
A2 & A3 & A4& A5	Degraded performance: define the behaviour of the gate in case of power off, of electrical shutdown… Shall e-gate have a power supply and/or a mechanical solution?	To help operators of ABC To easily communicate the passenger what will be done in case of degraded case	A combination of suppliers and border agencies/end-users, plus independent academics	Suppliers and purchasers	Handle degraded case
	TECHNICAL STANDARDS AREA: Safety design in automated barrier systems RECOMMENDED PROCEDURE AREA: Fall-back procedures in case of gate failure **PRIORITY: 2** The group agrees that most likely, a standard or recommended practice is already in place, but maybe not a European one. A good basis for this would be the Frontex document on operational best practice. The group agreed that such a standard will have a high impact (so priority 1 or 2), but there was a discussion on the difficulty of implementation. It might be less complicated on technical level, but might be more complicated on procedural level. The group finally settled with priority 2 and noted that the level of difficulty needs to be checked later. *FRONTEX: As proposals A2, A3, A4 and A5 are all similar (what to do in case of emergency/exceptional behaviour), all proposals are categorised in the same priority area. The standardisation of operational procedures should be out of the scope of this exercise. There is legislation in place, both at the EU and at the national level, establishing how border checks should be carried out. If an ABC system fails, travellers are redirected to manual control booths so the situation is no different than for "traditional" manual border checks.* *Operational procedures should be discussed by border management authorities in a different forum (e.g. Council WP). This is a subject for policy-makers.*				
A3	Emergency communication: define the way a passenger can ask and receive help	Safety	Suppliers, border agencies, Frontex, ICAO, IATA, advisors on special needs, end users, academics	Suppliers and purchasers	Handle emergency case
	TECHNICAL STANDARDS AREA: Safety design in automated barrier systems RECOMMENDED PROCEDURE AREA: Monitoring of ABC operation PRIORITY: 2 See A2				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
A4	Safety button : Define the role of a button in case of : - alarm (ex: passenger wants help) - panic (ex: passenger wants to go out quickly) - safety (ex: fire)	Security	Suppliers, border agencies, Frontex, ICAO, IATA, advisors on special needs, end users, academics	Suppliers and purchasers	Handle abnormal situation
	TECHNICAL STANDARDS AREA: RECOMMENDED PROCEDURE AREA: PRIORITY: 2 See A2	Safety design in automated barrier systems Monitoring of ABC operation			
A5	Environnement condition: Temperature, humidity, air pressure, dust, sand, salinity.	Reliability	Suppliers, border agencies, Frontex, ICAO, IATA, advisors on special needs, end users, academics	Suppliers and purchasers	Use ABC on different type of point of entry (land, sea, air)
	TECHNICAL STANDARDS AREA: RECOMMENDED PROCEDURE AREA: PRIORITY: 2 See A2	Operating environment parameters for safe and effective operation			
A6 See A21	To establish standards and parameters for liveness detection and anti-spoofing capability for biometrics embedded in automated border control systems	Operators of ABC systems are seldom absolutely clear about the meaning of suppliers' claims on liveness detection and resistance to spoofing. Clear performance standards, where possible, need to be established and published.	A combination of suppliers and border agencies/end-users, plus independent academics	Suppliers and purchasers	A published standard, compliance to which can be independently verified, which informs purchasers and managers of ABC systems as the performance to be expected – and relied upon – from their products.
	TECHNICAL STANDARDS AREA: RECOMMENDED PROCEDURE AREA: PRIORITY: none JTC 1/SC 37 Biometrics is currently developing this standard, so probably no need for this project to address this issue. Document in development: ISO/IEC WD 30107 Anti-Spoofing and Liveness Detection Techniques	Effectiveness against subversion by fraudulent presentation of biometric sample			

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
A7	To establish EU standards and parameters for cargo screening and monitoring embedded in automated border and customs control systems and checkpoints	Currently there are no common EU standard(s) and radiation safety regulations for X-ray screening systems, which could simultaneously operate back-/forward-scattering and dual view X-ray. Local regulations in EU member states vary and prohibit the “drive-through” configuration, for instance. This problem has appeared to prevent using of such technologies together even the end user desperately wishes.	A combination of suppliers and CBP agencies/end-users, radiation safety authorities, plus independent academics	Suppliers and purchasers	A published standard, compliance to which can be independently verified, which informs purchasers and managers of ABC systems as the performance to be expected – and relied upon.
	TECHNICAL STANDARDS AREA: Safety design in automated barrier systems Safe dose level for non-medical radiation RECOMMENDED PROCEDURE AREA: PRIORITY: none Cargo is not part of ABC systems. It does not fall in the scope of this work. This proposal will therefore not be addressed.				
A8	To design a common schedule of requirements for ABC systems	To guarantee a specified EU-level of performance and quality of the ABC system	Border-agencies / end-user / ICT-technicians	Suppliers, developers	Standardisation in the ABC-systems and level of quality
	TECHNICAL STANDARDS AREA: Common requirements set for ABC RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: none CEN/TC 224/WG18 is already addressing this, but only for airport environment. The WG does plan to extend this work to land and sea in the future. This proposal will therefore not be addressed in this project but the EU-funded ‘FastPass’ project will do so.				
A9	~~To discuss a common method of biometric identification which will be used in all ABC systems biometric framework~~ Adjustment of the proposal: a biometric framework and biometric performance assessment to be used in all ABC systems.	To come to one solution of identifying the passenger.	Biometric experts	End-users, passengers	Standardized method of identification. To simplify the using of the ABC-system for passengers.
	TECHNICAL STANDARDS AREA: Common requirements set for ABC Common political approach to border control Update of ICAO 9303 - travel documents RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: 2				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	It is not so much about to come to one technical solution, but to develop a biometric framework. Here it is also important to take biometric performance assessment into account. In addition, there is the issue of interoperability between systems in different EU member states. The EU 'Smart Borders, initiative will deepen don a certain degree of interoperability between MS systems and this will require a common 'Smart Borders' standard – somewhere between ISO/IEE/CEN specific standards and Frontex technical best practice. In view of the importance but non-urgency, further consideration at priority 2. *FRONTEX: It is very unclear what this means. What it is meant by "biometric framework"? What is a "Smart Borders standard"? As this stands now, it is not easy to see what is the issue to be addressed or the action proposed. Are you referring to biometric thresholds? If this is the case, there cannot be a single one although there could be a range. As background, in the "Smart Borders" initiative the European Commission proposes the creation of a Registered Traveller Programme for Third Country Nationals based on fingerprints. Registered Travellers could then go through the border by using ABC in those Border Crossing Points where such systems are available. The programme would be "interoperable" in the sense that it will be European, and therefore common to all MSs.*				
A10	Develop a European standard set for end-to-end tests	To guarantee a specified EU-level of performance and quality of the ABC system	Border-agencies / end-user / ICT-technicians	Testers / end-users	Standardisation in the methods of testing the ABC-systems and level of quality
	TECHNICAL STANDARDS AREA: Common tests for ABC systems Common ABC performance standards Safety design in automated barrier systems RECOMMENDED PROCEDURE AREA: PRIORITY: 4 The question was asked what end-to-end tests are. The proposal regards common test procedures, to be able to rely on tests done elsewhere (so you do not need to do all tests yourself). End-to-end is assumed to be considered the whole process of testing. There is a discussion on whether the proposal is a priority 2 or 4. As there are already test methods in place, this proposal is considered "good to have", but will have a lower impact/is of lower priority compared to other proposals.				
A11 & A12	Is there a need for harmonisation and standardisation on mobile biometrics systems in Europe (e.g. ABC, police verification systems, visa inspection systems)?	For flexibility in order to support temporary border set-ups, land border controls, …	CEN/TC224/WG18	M.S	An harmonization of mobile ABC biometrics system in E.U.
	TECHNICAL STANDARDS AREA: Common tests for ABC systems Common ABC performance standards Safety design in automated barrier systems Effectiveness against subversion by fraudulent presentation of biometric sample Operating environment parameters for safe and effective operation RECOMMENDED PROCEDURE AREA: PRIORITY: none Currently a NWIP is out for voting within CEN/TC 224/WG 18. There is a discussion on what is 'mobile' ABC. Also a discussion on whether a mobile/portable device is considered to be "automated" (so is it actually ABC then?). (An example was given: the idea is that with such a mobile system, the police for example can go to the queue instead of the queue waiting for the police.)				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	Furthermore a discussion on whether this falls within the scope of border control. Some do not think this is within the scope as this proposal is discussing something within a member state rather than between member states. *FRONTEX: Biometric checks using mobile devices are also taking place in a border control situation –e.g. VIS checks. This argument is not valid* There is a need for such a proposal, but the group decides it is not within this specific scope. The proposer is however encouraged to send more information and explanation to the project expert so this will be taken into account in the report.				
A12	A standard for mobile ABC (similar to CEN TC224 WG18 in ABC). FRONTEX: It is not ABC per se but the use of mobile devices for biometric identification and verification purposes (and this would indeed be interesting)	There are in the market mobile systems performing in a similar way than an ABC. Some EU borders are very permeable and some mobile systems could be needed. Also, Schengen borders can be avoided in some circumstances, so mobile systems could be used in these situations.	A combination of suppliers and border agencies/end-users, plus independent academics	Suppliers in building new systems; end users in specifying requirements for systems.	A published standard. Increased the market.
	TECHNICAL STANDARDS AREA: Common tests for ABC systems Common ABC performance standards Safety design in automated barrier systems Effectiveness against subversion by fraudulent presentation of biometric sample Operating environment parameters for safe and effective operation RECOMMENDED PROCEDURE AREA: PRIORITY: none See A11				
A13	Development of a minimal common set of security features for passports	One of the problems for ABC is the read out of ePassports. This should be harmonized anyhow for all EU-passports	A combination of suppliers and the member-states	Suppliers	Faster readout of passports Minimum level of security achieved.
	TECHNICAL STANDARDS AREA: Update of ICAO 9303 - travel documents RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: 2 On this issue political and economic issues are involved. It is an ICAO responsibility (9303). FRONTEX has recommended procedures/practices and guidelines (for chips in certificates). It is all about security features, physical features etc. (these last are different). ABC-systems are interested in the physical features. The group agrees that there is a piece of work to be done. Chris will check if this means work for FRONTEX or a national standard body. *FRONTEX: This is not the case. Frontex has published a study on the security of e-Passports and also raised the issue of certificate checks/ exchange in a number of occasions and with different stakeholders. The input received from MSs border management authorities indicate that difficulties concerning certificate exchange and distribution are impacting the performance of ABC systems. Last year Frontex drafted a "discussion paper" on this issue. The ABC Best Practice Guidelines emphasise the importance of having up-to-date certificates. However, Frontex has not produced any guidelines or procedures on certificate exchange as this is not under its mandate.* *Moreover, this is an area where the European Commission (DG HOME) should have a say as currently certificate exchange takes place under the umbrella of the Article 6 Committee. This was stressed several times during the Workshop. – Frontex. Not a task for Frontex or for a national standardisation body.*				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
A14	Establishment of standardization of interfaces	To achieve exchangeability of modules (e.g. passport reader)	Suppliers and integrators	Integrators	Plug-and-play of components Reduced costs for procurement and operation
	TECHNICAL STANDARDS AREA: Data interchange standards Hardware interconnectivity protocols RECOMMENDED PROCEDURE AREA: PRIORITY: 3 This issue is about different components in an ABC-system. Is there an interface needed for document readers? Is there a standard for transporting the information data from a passport reader to the gate system? Standards should not block innovation! They must describe a minimum! It is an interesting issue, especially for developments in the future. It will be important for 'Smart Borders' and also when components in existing ABC systems are replaced with units from other suppliers. Standards will work to the advantage of all but it is not a high priority at the moment.				
A15	Increase the size of the group of laboratories/institutions certified to undertake performance and security testing.	At present, there are very few test houses in the EU who would be able to carry out such highly specialised testing (1-3 national information assurance authorities, 3-4 independent test houses/universities)	ERNCIP TG on Applied Biometrics for CIP has been tasked with assessing the current status of the market, and may be able to provide some support to EC initiatives. Materials (e.g. guidance, training etc) and mentoring will be required for new entrants into the market	System suppliers and authorities deploying and maintaining ABC systems	Wider recognition of the need for, and ability to test, ABC systems deployed in the EU
	TECHNICAL STANDARDS AREA: Certification for testing agencies Common tests for ABC systems Common ABC performance standards Safety design in automated barrier systems RECOMMENDED PROCEDURE AREA: PRIORITY: none The group agreed that this issue is out of scope.				
A16	Development of standards profiles for testing the security and performance of ABC systems.	Although there are international standards for testing biometric components and systems (e.g. vocabulary in ISO/IEC 2382-37, conformance testing to data interchange formats in the 29109-x series and for biometric performance testing in the 19795-x series) and best practices (e.g. from Frontex), these are generic standards, not designed specifically for ABC systems. ISO SC37 WG4 develops Biometric Profiles in the 24713-x series which should help address this requirement.	CEN TC224 WG18 ERNCIP TG on Applied Biometrics for CIP has identified development of testing of ABC gates as one of its key priority areas. Although the Thematic Group will undertake some work in calendar years 2013-14 directed to the introduction of CEN standards, this will	Test houses, system suppliers, authorities deploying and maintaining ABC systems	Common approach to specification and testing of systems, to ensure uniform security operations across the borders of the EU, clear

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
		Vocabulary and metrics for the reporting of performance of systems may need to be developed as part of this profile. Processes for testing of security parameters in the biometric elements need specific advice in order to ensure conformance to data protection laws.	be on a voluntary basis. Work could be accelerated if funds were made available to individuals/organisations for the development and demonstration of biometric profile standards		specifications in the procurement of ABC systems, etc
	TECHNICAL STANDARDS AREA: Certification for testing agencies Common tests for ABC systems Common ABC performance standards Safety design in automated barrier systems RECOMMENDED PROCEDURE AREA: PRIORITY: no score This issue was also discussed in group B. The group agrees this issue has to be combined with the issue and outcome of group B.				
A17	Development of a systems engineering handbook/Body of Knowledge on integrated border security systems (including ABC gates, improved throughput, customs control)	Currently systems are engineered to address specific single bundles of requirements rather than as an integrated process through which travellers pass in the most effective way, and port/border authorities are assured of required level of secure control, etc. A systems engineering approach, based upon best practices, would enable individual authorities and integrators to develop more cost-effective and user-friendly systems.	Specialist professional services organisation on contract to Frontex. The aim would be to develop a registered scheme, allowing those adhering to the approach to gain accreditation.	System suppliers and integrators,, authorities deploying and maintaining ABC systems, ports at which the ABC system is installed	Better engineered systems at ports should result in optimised cost-effective designs with a more pleasant experience for the traveller. Integrators and suppliers of such systems may be able to gain higher value business through conformance with such a scheme.
	TECHNICAL STANDARDS AREA: Common ABC performance standards Safety design in automated barrier systems Effectiveness against subversion by fraudulent presentation of biometric sample Operating environment parameters for safe and effective operation RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: none There are current leading documents by FRONTEX, so this is an issue for them. *FRONTEX: Not sure what this refers to … Customs is outside the mandate of Frontex. What Frontex has produced are technical and operational best practice guidelines on ABC systems*				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
A18	Thermal capture of traveller. This component can be an optional equipment that can be mounted on special occasion. (pandemic alarm)	For sanitary purpose, a thermal measure of the traveller can detect potential contamination risk in case of major pandemic alarm.	A combination of suppliers and border agencies/end-users	Suppliers and purchasers , end users in specifying requirements for systems.	Reduce staffing for thermal measure in airport of passenger and automated the detection. In addition, this information may be used for behaviour analysis.
	TECHNICAL STANDARDS AREA: Human temperature sensing RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: out of scope Questions: - Should this be a subject for an ABC-system? (seems interesting) - Is there already a standard on this subject? It is part of the conversation with the World Health Organisation. It is possible to introduce it as an option in the ABC infrastructure, but we need to consider what to do if an ABC-system is not used by a traveller. The group agrees that this issue is out of scope.				
A19	Performance fingerprint sensor in case of dirt.	With a high flow of traveller, some sweeting, some with greased fingerprint from lobby or meal, it may not be easy to clean regularly the fingerprint sensor. Therefore, the fingerprint sensor shall support a certain level of defined dirt (grease, perspiration …).	A combination of suppliers and border agencies/end-users	Suppliers and purchasers	Reduce the cleaning maintenance of fingerprint sensor, which is not always possible when major arrival and improve the performance in case of dirt, to prevent false rejection and ensure sufficient level of matching when using the ABC.
	TECHNICAL STANDARDS AREA: Biometric capture systems RECOMMENDED PROCEDURE AREA: Common operational procedures				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	PRIORITY: 2 Is there a standard for catching fingerprints? This was also part of the discussion the day before. This issue has to be combined with the issues A5, A6 and A9! It is already used at the airports of Singapore and Hong Kong (experiences?) We have to keep in mind that this is also part of the maintenance of the system.				
A20	To establish standards and performance parameters for 'on-the-fly' biometric verification (i.e. biometric capture with the passenger not having a physical contact with the biometric device and with a very fast biometric capture up to the point of not having to stop) in automated border control (ABC) solutions.	The use of such biometric techniques is meant to expedite transactions and thus improve flow management with a high level of security linked to biometrics. In order to grant possibility to compare accuracy and speed performances and to grant minimum levels of performances, standards and metrics are needed.	A combination of suppliers and border agencies/end-users, plus independent academics and representative organizations of stakeholders.	Vendors and purchasers. Regulation entities potentially.	Improving ABC solutions in terms of throughput and hence improving facilitation of passengers and operation for the air transportation stakeholders and the border control stakeholders
	TECHNICAL STANDARDS AREA: Biometric capture systems RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: no score This item is a responsibility of the vendors. There are standards on what, where and how it is captured, but not when (distance)! The group agrees that It is an interesting subject but not relevant for the time being.				
A21	To establish standards and parameters for liveness detection and anti-spoofing capability for biometrics embedded in automated border control systems	Operators of ABC systems are seldom absolutely clear about the meaning of suppliers' claims on liveness detection and resistance to spoofing. Clear performance standards, where possible, need to be established and published.	A combination of suppliers and border agencies/end-users, plus independent academics	Suppliers and purchasers	A published standard, compliance to which can be independently verified, which informs purchasers and managers of ABC systems as the performance to be expected – and relied upon – from their products.
See A6	TECHNICAL STANDARDS AREA: Biometric capture systems RECOMMENDED PROCEDURE AREA: Common operational procedures Registered Travel Scheme PRIORITY: no score				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	This is the same as subject A6.				
A22	Standard for performance, testing and mounting of terahertz detectors in conjunction with passenger queues and movement	No such standard exists and such sensors may well be placed within or near ABC systems as part of an integrated contraband/security detection system	A standards body with assistance from academics, suppliers and R&D agencies.	Agencies specifying such an add-on; suppliers	
	TECHNICAL STANDARDS AREA: RECOMMENDED PROCEDURE AREA: PRIORITY: no score It is the same subject area and priority as A18.	Human temperature sensing Passive terahertz radiation Common operational procedures Registered Travel Scheme			
A23	To develop a standard on a methodology to select and design the optimum biometric system for a given border crossing or immigration control context. Essentially, following a set of established procedures that provide consistency should improve decision making when stakeholders have to consider many complex factors.	Stakeholders, which include border control police, airport authorities, airlines and customs etc, need to consider many complex and interrelated factors in order to select and configure biometric systems that meet all stakeholder objectives and operational requirements, e.g. environmental and ergonomic. A methodology to assist a programme to consider these factors in a systematic and structured manner should improve decision making on selecting and configuring the optimal biometric system. An additional benefit is that it will provide a decision trail on such decisions.	A combination of Frontex, professional services suppliers and border agencies/end-users, plus independent academics. It should specifically exclude biometric system suppliers or system integrators.	Border Control Agencies will use this methodology as a systematic and structured approach to select the optimal biometric system. Currently, there are development methodologies, e.g. RUP, and programme methodologies, e.g. Prince2; however, none of them are specifically tailored to help stakeholders' select biometric systems.	Stakeholders will be in a better position to understand a range of stakeholder objectives and operational requirements to then consider the various biometric solution options. Improving decision-making should reduce programme costs and improve delivery timescales. Selecting the optimal biometric system should also reduce operating costs and issues. Many issues occur because

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
					insufficient regard is paid to understanding stakeholder objective and operational requirements. Technology suppliers focus their attention on selling their product and not taking an independent view on the stakeholders' challenges.
	TECHNICAL STANDARDS AREA: Drafting of technical specifications Business cases RECOMMENDED PROCEDURE AREA: Common project initiation standards Stakeholder management PRIORITY: 3 This is about a standard methodology for designing an ABC-system. It is a kind of blue-print for people designing these systems. The group agrees that there should be a best practice guideline. Task for FRONTEX Make sure all relevant elements are in it. Make sure all stakeholders are involved. It is not a technical thing but a business model! *FRONTEX:: ? The meaning of this is not clear. However, if this refers to the decision-making framework and cost and benefit analysis for different stakeholders, indeed Frontex has developed certain capability tools to support decision-making, including a Cost Benefit Analysis framework and operational research models, which are being used by national authorities, airports and vendors. This could be used as a basis for a common, harmonised framework.* *Note also that other stakeholders are doing work in this area. For example, ACI and IATA are developing an implementation guide for ABC from the perspective of carriers and airport operators.* *TONY PALMER: The third comment of "business models" suggests that is a misunderstanding regarding the purpose of developing a standard for a methodology to select the optimal ABC.* *1. A better description is offered.* *"A systematic method to select the optimal ABC. The methodology acts an aide memoire tool to assist stakeholders consider the technical and operational factors that need in selecting and deploying an ABC." In a nutshell a method, describes how a task may be achieved using a systematic process."* *The benefits to the EU and Frontex are that the method would provide consistency in selecting ABC for each context rather than be left to the experts, which may be employed by suppliers.*				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	The benefits to Border Control Police are that they would not have to rely so heavily on these experts. A systematic approach should also assist decision-making and provide an audit trail as to how the decision was arrived at. *2. It is a relatively quick win and should get a higher priority because there are existing scientific papers on such methodologies.* *May I suggest that references are made to my published papers:* *1. Criteria to evaluate Automated Personal Identification Mechanisms* *{ http://www.sciencedirect.com/science/article/pii/S016740480800045X}* *and* *2. Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA)* *{http://www.sciencedirect.com/science/article/pii/S0167404810000325}* *in Computers & Security as immediately available inputs into the development of a standard or guidelines-*				

B Recommended Operational & Project Practices

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
B1	To establish a standard for measuring the throughput of different types of e-Gates	Today, every vendor has the freedom to establish throughput (numbers of passengers process per time unit) criteria, sometimes subject to assumptions that make an objective comparison very difficult.	A combination of suppliers and Frontex, supported by border agencies and independent advisors	Governments, for objectively comparing performances of different systems and for accurate capacity planning.	A published standard, compliance to which can be independently verified, which informs purchasers and managers of ABC systems as the throughput to be expected – and relied upon for capacity planning.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: 2 Chris gave an example; Suppose you get an offer from a supplier and you ask 'how quick is your system' and they say '8 seconds', the question is '8 seconds of what', from where to where?. It is important to know the public perceive this issue and also how operational research experts/statisticians would define it. Perhaps this subject is more for a practical guideline to define the 'transaction cycle' for ABC so that claims by suppliers can be measured against it. *FRONTEX: Note that there are different topologies in place and that it is not possible to compare the end-to-end duration of a transaction across some of them (e.g. two step, where there is a physical distance between the passport reader and the biometric capture and the e-Gate, and one step).* *Moreover, it is up to the border management authority to determine the required performance levels through their service level agreements with the suppliers. This was noted during the Workshop, but it is not reflected here.*				
B2	Define operational standards for the use of iris technology in ABC systems	Several RU member states are keeping the option open for using iris recognition in the medium term. This	Suppliers, Frontex, advisors and academics	Governments for objectively defining requirements of	Positive: The availability of a standard for using iris technology at the border will allow for predictable

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
		is probably inspired by the EU plans to allow for a Registered Traveller Program, processing qualified third country nationals.		future border management systems	use of iris in coming RTP systems
	TECHNICAL STANDARDS AREA: Common performance standards for ABC *Performance standards for iris biometric systems* *RECOMMENDED PROCEDURE AREA: Common operational procedures* *Registered Travel Scheme* *PRIORITY: 4* *The group believes that this won't be part of an ABC-system as currently defined but could be used in support of the 'official' face and fingerprint for registered travel or other boarding or border control systems used by particular airports or member states. A 'nice to have' but not a priority. The UK's iris ABC will be taken out of service within the next year or so.* *FRONTEX: Also, note that recommendations for use of iris have already been drafted by TC224/WG18*				
B3	Is there a need for biometrics to be embedded in breeder documents? If yes how and which biometrics?	To stop fraud	CEN/TC224/WG18	M.S	To reduce fraud for travel documents
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: no score The group considered that this subject is more about the documents which are used in border security - and these documents are not within the scope of the project.				
B4	Is there a need for a harmonisation of biometric sample quality embedded in e-passports (e.g. face, fingerprints)?	Harmonisation of identity checks at the border especially for ABC	CEN/TC224/WG18	M.S	To reduce false rejection rate when crossing borders (ABC)
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: 2 The group agrees that the word 'harmonisation' in de 3rd column is not a fortunate word. Is there already an ISO-standard? (only structure, not the content or the quality). The group agrees to use the ISO-standards; the given priority is to indicate the pressure on the work that has to be done.				
B5	Is there a need for better facilitation of e-passports related certificates especially in ABC context (e.g. passport validation certificates and EAC)?	Convenience for the travellers and authorities.	CEN/TC224/WG18	M.S	Facilitation for EU citizens to access any EU/Schengen border

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: 2 Perhaps there has already some work been done on a PKD for management of digital certificates but that hasn't been very effective. A standardised scheme would help. Some members of the group mention that there is work in progress. All agree that is has a priority but not for us. The project to research this issue. *FRONTEX: See comments to A 13. The standardisation roadmap could raise the fact that this is a priority that required further action*				
B6	Is there a need to develop the actual TS document on ABC made by the CEN TC224/WG18 to an EN? If yes, is it for all EU or Schengen only?	Convenience for the travellers and authorities.	CEN/TC224/WG18	M.S.	An harmonization of the ABC system in E.U.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures PRIORITY: 1 The group is unknown with the scope of the work of CEN/TC224/WG18. Is it about interoperability of biometrics? They all agree that to develop the mentioned document there has to be some work done. Clarification with CEN required.				
B7	Establishment of a minimal technical set of security checks for automated border control (eg. Passport readout, person separation, left luggage detection, biometrics verification of live and passport image against chip image, liveness detection)	With the minimal set, a minimum standard of security for all border crossing points can be established, This is particular useful, wherever common borders (Schengen) is concerned.	A combination of suppliers and border agencies/end-users, plus independent academics	Suppliers and border guards	A published European standard
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 1 This subject is about the functionality of ABC-systems, not about the security of these systems. Part of this is covered by FRONTEX guidelines. There is a relation with the subjects B10 (and B15 and B16) and a possible connection with B6. There is a difference between products and systems! *FRONTEX: Again, it is up to the border management authorities to define technical requirements to meet the requisite security levels. It is not up to industry to define them.*				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
B8	Establishment of a standard which facilitates an independent security certification process for ABC (which are controlled on a regularly basis)	Technically nearly everything is possible but in the end nobody knows which checks are enabled and independent groups should certify the implementation	End users and Frontex	Suppliers and border guards	Increasing security due to the "better understanding" of the ABCs
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 1 This subject is related to B7. One of the Dutch delegates came up with a new proposal (received 06-04-2013, highlighted in green) This should be based upon/ cover: - the risk model of Frontex for (A)BC - list of vulnerabilities/risks - list of security objectives - derived (security) functional requirements - development of a certification scheme which covers accreditation and certification processes, incl. re-certification after substantial changes have been made post-deployment - certifying organisations should be accredited - certification should demonstrate by testing that the requirements have been met to the appropriate level *FRONTEX: Frontex cannot be an independent security certification body (explained during the Workshop)*				
B9	Standard or TS on usability requirements in ABC components and systems, ways of testing usability, and assessing the acceptance and promotion/marketing of ABC systems	Based upon experience gained in the EU and elsewhere, to develop best practices and approaches, building on the NIST *Biometrics and Usability* team.	Either Frontex or a specific organisation/institute tasked by Frontex	Component and system suppliers. Authorities deploying and maintaining ABC systems	Impetus to suppliers to develop components and systems which have usability at their heart. Improved market for EU products and systems..
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score *FRONTEX: It was mentioned during the Workshop that the JRC could have some role in testing usability*				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
B10	Development of new security standards which facilitate and govern certification approaches (standards) for ABC systems	Certification that a given installation meets specified security requirements is problematic in mixed IT/physical security installations such as ABC systems. Common Criteria certification in respect of IT security (in accordance with ISO/IEC 15408) is both expensive and time consuming, as well as somewhat inflexible in respect of system upgrades	JRC at Ispra has started preparations for an international conference on alternatives to Common Criteria, and, together with ENISA, would be best placed to continue this work	Test houses, system suppliers, authorities deploying and maintaining ABC systems	Common approach to specification and testing of systems, to ensure uniform security operations across the borders of the EU, clear specifications in the procurement of ABC systems, etc
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score				
B11	Development of training standards for officials at secondary inspection following failure at biometric gates (especially for gates using face recognition)	If the failure is due to failure to match with the photograph in the passport, the policy in MS may advise on techniques to visually compare the person with the photograph.	Standards for human facial comparison are being developed internationally by FISWG, http://www.fiswg.org , and training standards for image-to-person comparison could be proposed by members of this group	Authorities deploying and maintaining ABC systems	Common approach to ensure uniform security operations across the borders of the EU
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 3 The description isn´t correct/complete. FRONTEX will deliver new text for this proposal! The subject is part of ID-checking and part of procedure. E.g. 'what do I do in case of …' and 'what should I do in case of …'. It is also part of European and national legislation. *FRONTEX: See comments to A2. On a different note, Frontex is currently exploring in cooperation with the MSs the possibility to develop a training on vulnerability assessment of biometric systems with a specific focus on ABC.*				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
B12	Collation of best practice at enrolment for ePassports and the standardisation of quality enrolment and reporting for fingerprint collection, together with a mechanism for cross-national evaluation (cp. Brussels Interoperability Group)	Countries across the EU are enrolling biometric characteristics using different equipment, processes and quality metrics. In the absence of a common standard for the quality of fingerprint images, and the necessary controls to monitor this on a European basis, future ABC systems using fingerprints will operate sub-optimally	CEN TC224 WG18	Passport and identity card issuing authorities	Better performance of future, fingerprint-enabled ABC systems
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 2 This subject has great similarity with B3. The group agrees to merge this subject with B6. It is more a subject for passports than for ABC-systems.				
B13	Establish set of standards for test levels in CBRNE at border crossings including sensor operating temperature range, humidity, expected level of training, calibration, evidence traceability.	Many existing sensors do not work outside the laboratory because the original specification was inadequate for what they had to meet. Research has to produce product that is easy to use and cost effective	Research institutes, manufacturers, border agencies and Frontex.	Border guards and security agencies	Immediate ease of use, fit for purpose, deter terrorists and smugglers
	TECHNICAL STANDARDS AREA: Common performance standards for ABC Fissile material detector standards RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score				
B14	Outline a specification for detecting of CBRN (from CBRNE) at a standoff distance and linked to standard control systems ACROSS borders	Emergencies concerning CBRN will cross borders by road, rail, river and air. There has to be a high speed detection system that allows the free passage of people and cargo but linked to national control centres	Suppliers, research institutes, border agencies and Frontex.	Suppliers in building new systems; end users in specifying requirements for systems.	100% checking of all those moving through a border crossing with minimal interruption
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
B15	Design a specification for use of RFID devices in cargo at border crossings for standoff interrogation by portable readers either stationary or moving	Border guards need a faster way to check on cargo against the manifest	Suppliers, research institutes, border agencies and Frontex.	Suppliers in building new systems; end users in specifying requirements for systems.	100% checking of all those moving through a border crossing with minimal interruption
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score The group agrees that this subject is out of scope.				
B16	Standards for the use of embedded RFID in transport tickets (Air, sea, river, train, road)	Cross check of ticket details to validate user with form of travel. Especially needed in airports to provide a secure corridor	Suppliers, research institutes, border agencies and Frontex.	Suppliers in building new systems; end users in specifying requirements for systems.	Security within airports and high speed rail stations.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score Are we allowed to collect this kind of information in ABC-systems?				
B17	To establish standards certifiable according a common European framework	Implementations of standards by suppliers should be able to pass a certification process in order to sure (by independent laboratory) that the conditions defined in standards are really incorporates to the products (hardware, software and process)	A combination of suppliers and border agencies/end-users, plus independent laboratories	Suppliers and purchasers	A published standard, compliance to which can be independently verified, which informs purchasers and managers of ABC systems and biometrics as the performance, security and INTEROPERABILITY to be expected – and relied upon – from their products.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score This subject has to be combined with other subjects concerning certification.				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
B18	Environmental working condition to use the same equipment for all type of Point of Entry (i.e. Seaport, land border, airport…)	As ABC is not limited to airport and can be used in various environment with different constraints, it shall comply to a minimum set of conditions for security usage according to environment (Temperature, humidity, sea salt water …). At least different sets of constraints need to be defined by category of environment	A combination of suppliers and border agencies/end-users, plus independent academics	Suppliers and purchasers	A published standard, compliance to which can be independently verified, which informs purchasers and managers of ABC systems as the performance to be expected – and relied upon – from their products.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score This subject is generic or specifically for certain circumstances. What works in Greece can give problems in Finland. This seems to be a subject for FRONTEX. *FRONTEX: Is it? Frontex does not have either the capacity or the expertise. Frontex is not mandated to develop standards*				
B19	Full body or upper half body camera for behavioural analysis.	Capture the images to analyse body languages and behaviours to enables behaviour analysis by software.	Suppliers, border agencies, Frontex, IATA, advisors on special needs, end users, academics.	Suppliers and purchasers	When part of the border control officer efficiency is based on behaviour analysis, some case/element can be automated to detect specific behaviour and raise specific alarm for further control by border officer or flag somebody for custom.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score The group wonders if we are allowed to use this in ABC-systems.				
B20	A standard set of guidance – in terms of vocabulary (in multiple languages), iconography, text and display methodology and format – for passengers using ABC systems of similar types.	Using ABC systems should be intuitive and simple, much as ATM machines have become the routine and most convenient way to obtain cash from banks.	Suppliers, border agencies, Frontex, ICAO, IATA, advisors on special needs, end users, academics.	Suppliers in building new systems; end users in specifying requirements for systems.	Beneficial – making systems much easier to use for both first-time and regular users; also to reduce the amount of assistance required from carrier and port staff.

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 1 This is a good idea. There are some developments in ISO and ACI (Airports Council International) FRONTEX has already information about the use of multiple languages and positions of the passports that is being used/is being developed.				

C Information and Privacy

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
C1	A coherent framework for addressing Societal Implications, fundamental rights and privacy issues (privacy by design and privacy by default) of ABC systems and Biometric technologies.	Developing and using ABC systems, and their standardisation, may have wide societal implications. Horizon 2020 emphasises that societal and fundamental rights impact should be assessed before and during R&D and to make societal impact checking more systematic. Given the complexity of products, and variation in practices and societal issues among EU member states, there is a need for a coherent framework to enable effective and relatively standardised societal impact assessment at all stages. The societal impact of standardisation of ABC and Biometrics, as well as the development of these, needs to be better understood.	Multi-disciplinary collaboration between social scientists, engineers, end-users and policy agencies at national and EU levels.	Policy makers, industry, suppliers, end-users and other stakeholders.	A coherent and efficient framework for assessing societal implications in ABC and Biometrics at all stages (R&D, Procurement, deployment and use) to enable effective and appropriate understanding of societal implications.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance Privacy and Data protection in ABC Systems PRIORITY 2 It is difficult to translate these legal considerations but overall, it is a good proposal – to be further considered. Privacy by design is of relevance especially in the ABC context .FRONTEX pointed out that other EU agencies (ENISA and Eu agenc for fundamental rights) have asked them to contribute in streamlining a policy on this matter. at this time, there are many differences among Member states on what these two concept would mean. CEN/TC 224 approach is to develop guidelines focusing on the user and not the manufacturer or security technology developer. It is not possible to regulate the technology but the				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	data which comes before the product or the component is created. The experts in the Netherlands concluded that privacy is a societal value of non –exposure of personal data /info and this is difficult to quantify a concept, while data protection is more measurable and should be translated into requirements. It is worth doing it upon the publication of the new regulation on data protection. Some experts pointed out the need to address data retention in the ABC context. EC is currently investigating whether a management system standard will be able to address this issue. This should be implemented in all security technologies/equipment. in first instance, the Commission will do some case studies to investigate how industry has implemented this concepts in their own processes . *Mike Bourne:* *First, the classification of the proposal as priority 2: In the group discussions we came to the conclusion that this issue should be given priority 1 rather than 2. I guess it was more akin to a 1.5 priority. The issue here was that as an indicator of importance the proposal was a 1; but in terms of being a longer term project with some preliminary work needed it fits into 2. While I initially suggested 2 due to the longer term nature of the work, others, particularly Rasa, wanted to emphasise the overall importance by designating it as a 1.* *Second, while a lot of the discussion focussed on privacy by design and the current ambiguities of what this means the proposal is for a wider societal and rights framework. The inspiration for this proposal derives from the attached recent report for DG ENTR that suggests that all European funded security technology research projects include a dedicated work package on societal impact that conducts a series of societal impact reviews. This being the case I thought it useful to develop a coherent framework for the conduct of this through inter-disciplinary work and collaboration between companies, academics, end users and policy makers etc.* *Third, while the Dutch experts may have concluded that privacy is a value of non-exposure of personal data, when looking at the types of social and political controversies that have arisen in relation to other border security technologies, biometrics etc, it is clear to me that privacy goes far beyond this. I guess the clearest way to characterise this is that data protection pertains to ensuring that only authorised persons and agencies are able to access the data that is collected and used. Privacy, however, pertains to the wider socio-technical system in which ABM and other technologies are embedded. It relates to concerns about what data is collected in the first place, how people consent to that collection and how informed that consent is; how the operationalization of such controls constricts or enables the time and space for decisions (such as eligibility for asylum); and so forth. As such it seeks to take into account the range of social and rights issues (including but not only legal issues) that arise in the use of technologies and to ensure that those issues are built in to the technologies in appropriate ways. The purpose of this proposed framework is to enable that assessment in a relatively straightforward way, and to ensure that similar issues and assessments are utilised and addressed across different technology development processes rather than a fragmented and ad hoc series of assessments of widely varying quality and impact.* *This of course raises a crucially important question of whether and how to take this forward in the framework of standardisation or through another process. My feeling is that the standardisation process offers considerable opportunities in this regard, and also that since there is a wider move towards such privacy by design and societal impact assessments it would be important for this standardisation process to ensure that it is attuned to those developments so that it creates a process that is not left behind or in need of amendment when those wider processes become clearer and stronger.* *Matthias Pocs: The group agreed to give this proposal priority 3 or 4. Please cross-check this if you are in doubt. The problems are that societal considerations are extremely difficult to translate into technical requirements. There is a variety of political, legal and social differences in the Member States which is nearly impossible to translate in a set of requirements.* *FRONTEX:* *Frontex noted that the FRA is taking the issue of ABC into consideration in particular from the point of view of data protection and non-discrimination (travellers with disabilities). Frontex has been in contact with them but they have not asked Frontex "to streamline a policy on the matter"* *Note that ABC systems do not retain any personal data of EU citizens. The only data which is stored is anonymised and kept for the purposes of quality control and statistics. The situation is different in RTPs, but then you have travellers which enrol voluntarily in the system so they agree for their data to be retained in a database*				
C2	A standard for data distribution	There are several problems with these server-client	Suppliers	Suppliers can use	Equipment can be easily

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	system especially for real-time video, camera operation, sensor data, etc. Using a data distribution DDS middleware allows real-time, bandwidth-optimized data transfer without relying on a server-client architecture. The proposal is to use a publisher-subscriber network. In the publish-subscribe model there is no central data server, hence no single point of failure. Instead, data flows directly from source to destination. Data sources put data onto the network (publish) as the data becomes available, tagging that data for receipt by all registered subscribers. Control elements that need data alert the data sources to their needs by registering with the data source as a subscriber.	architectures. One is that they have a single point of failure: the server. If it goes down the entire system collapses. Building failover redundancy is both difficult and costly in a client-server architecture. The central server also serves as a data bottleneck in the system because it must handle each piece of data twice: once to receive and once to send. Another problem with the client-server architecture is that it becomes increasingly difficult to modify, upgrade and maintain as the system becomes more complex.		these standard protocols for transmitting data and controlling the sensors.	exchanged between different locations. Operation of equipment can be managed via wide-area networks
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: none. No further consideration. This is too problematic. The way it is formulated it implies that the systems will not change in the next 10/ 20 years which is not likely to happen. Suppliers should always have a set of options from which they select the architecture(it is a matter of choice). A possible approach would be to focus on how data should be shared and how fast to change between one or another.				
C3	A system for a Shared Security	All border posts store their video information on local	Suppliers on basis of	Command Centres	Quicker reaction for data evaluation

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	Database in which data especially those of video sensors can be stored and disseminated.	servers. The information cannot be shared or taken for common Information Requests. The data cannot be curtailed for specific search requests in time frame and location. Time consuming evaluation in case of incident is happens.	STANAG 4609 and 4545	searching and evaluating data can use the Pull-Function to gain information from distributed locations	in case of incident
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: none. No further consideration. There is a need to have international standards on meta-data- this is currently done in ISO/TC 223. The standard is now published as ISO 22311:2012.				
C4	Is there a need for harmonisation of exchange of biometric data between member states/countries?	Facilitation of police exchange of data	CEN	Police/Europol, Member states	Facilitation of investigation, better cooperation between police forces
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance Privacy and Data protection in ABC Systems Biometric/biographic Data Exchange Standards for Border Control? PRIORITY: none. No further consideration. This is not a matter for standardization but for legislation. More likely to be addressed somehow when standardizing the ABC process and procedures.				
C5	Is there a need to develop guidance and /or rules for privacy preserving technical concept within standardisation?	There is a lack of guidance at the moment for implementing privacy by design	CEN/TC224/WG18	Industries	Better acceptance of security technologies by the public
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 1 or 2 This is linked with proposal C1. A list of security measures in this context will never be exhaustive. However, the process should be quickly standardized because there should be a common view on this matter. . In contrast to C1 the group agrees				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	CEN/TC 224 approach is to develop guidelines focusing on the manufacturer or security technology developer not the user. This proposal's innovation is to regulate the technology before the product or the component is created instead of regulating real-life data which is only processed after the beginning of the deployment. The Commission underlined Action 8 of its Security Industrial Policy. It planned to develop an ISO-9000-like quality standard that focuses on the process. The Commission expressed the need for input for Action 8. There is a connection between the proposal and Action 8. *Matthias Pocs: The group agreed to give this proposal priority 1. Please cross-check this if you are in doubt. The rationale is that this proposal aims to develop the process not the societal requirements which can be quickly implemented.*				
C6	e-VISA There are requirement specifications for multiple forms of electronic MRTD with biometrics but none for VISA. A standardised e-VISA may even be included in secure elements of NFC phones and might not require a physical printing.	The security of VISA should be aligned and raised to the same level as e-Passport or e-ID cards; particularly because they are used all together	National security agencies together with security corporations. Industry associations like NFC forum may play a role.	National printing houses, embassies and border control	Better harmonized level of security for VISAs. Independence of backbone network with all their privacy issues. The citizen gets in control of his ID and biometrics and the authority gets a secure and privacy friendly control mechanism
	TECHNICAL STANDARDS AREA: RECOMMENDED PROCEDURE AREA: PRIORITY: None. This is already standardized.	Common performance standards for ABC ICAO 9303 Common operational procedures ICAO/Frontex Operational Guidance EU VIS Operational Standards			
C7	A standard set how to use RFID enabled e-MRTD remotely on NFC-phones, e.g on the internet	e-MRTD provide a very secure and cost efficient way of personal identification that also allows dual use in a privacy friendly way. All what is missing are related standards	NFC industry together with IETF as internet standardization organisation	Citizen for secure identification on the internet. Public and private service providers including tax offices, universities etc.	There is a cost efficient way of re-using the already deployed e-MRTD for secure identification on the internet without the need to develop and deploy new ID schemes
	TECHNICAL STANDARDS AREA: RECOMMENDED PROCEDURE AREA: PRIORITY: 4 The proposal should be reformulated- just for the exit control. This is an opportunity in view of improved throughput.	Common performance standards for ABC ICAO 9303 NFC Data Storage and Transmission Common operational procedures ICAO/Frontex Operational Guidance			

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	Would not this imply infringement of data protection rules? Some suggested that this has nothing to do with the border control. It is not for short-term consideration, there are currently discussions on this subject at FRONTEX WG (liked to the new concept of virtual borders) but at a certain moment in time it would be worth doing it. *FRONTEX: This is not the case. Frontex is exploring the use of different technologies including mobile and portable technologies within the virtual border concept*				
C8	Travel ticket reading and control before entering automated border control unit. It shall work with official tickets, printed-paper or e-ticket on mobile device (i.e. smartphone).	Most travel document use 2D bare code (paper, ticket, smartphone or some still magnet stripe and can be automatically read. The captured travel information and linked with the traveller. It ensures the right to access border if the ticket is valid, and enable to track the impacted traveller in case of cancellation.	Suppliers, border agencies, Frontex, ICAO, IATA, end users, travel agencies.	Suppliers and purchasers	Linked the traveller with its travel ticket. Reduce the manual control of ticket to access border area. Pre-detection of potential traveller in case of cancellation of transportation mean. It shall support the ticket evolution linked which are more and more available on mobile devices.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 IATA Ticketing and Boarding Passes RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: None. Works is underway.				
C9	Define interfaces and use of international set of data to be used during document control (i.e. Interpol …).	During the automated border control, the travel document shall be automatically controlled. This control can use existing database provided by sub-parties such as Interpol SLTD, DialDoc. The use of those internationally recognised data will improve automated security control and ensure a common minimum level of control.	Suppliers, border agencies, Frontex, Interpol, other agencies providing control database, end users.	Suppliers in building new systems; end users in specifying requirements for systems.	Improve the automated control of travel document based on internationally recognised database. Ensure a common minimum-security control.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance Biometric/biographic Data Exchange Standards for Border Control? PRIORITY: None. This cannot be work to be done by standardization				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
C10	Security of data transmission between equipment and the ABC system and ABC personal data storage.	To comply with law related to data privacy such as area of freedom, security and justice.	Suppliers, border agencies, Frontex, advisors, end-users.	Suppliers in building new systems; end users in specifying requirements for systems.	Ensure segregation of captured data and secure communication of those data between all components of the ABC system. Ensure end-to-end security of the personal data of travellers.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: none Subject under discussion at FRONTEX WG (to be part of the technical guidelines ABC) and then the EC should enforce the mechanism. To be investigated the way the border certificates are registered – art 6 SIS II. PKIs need to be implemented as part of the ABC system. It should clearly defined what a secure system is, and then set up the requirements. Inter-SPOC testing is something that needs to be addressed separately. *FRONTEX: What does the SIS II have to do with certificate exchange? See comments on A13 and B5* *Olivier Monsacre: For C10, I had in my notes a comment about rewriting it and linking it to B7-B8*.				
C11	To develop a standard integrated set of operating and security requirements for deploying eMRTD inspection systems that perform cryptographic processing and biometric verification processing for eMRTDs with various ICAO/EU protocols, e.g. Passive Authentication, Extended Access Control, Supplementary Access Control etc. Also, it is important to state security requirements to minimise potential fraudulent activities relating to inspection systems, e.g. the introduction of bogus certificates. Travellers will also seek assurance that their biometric data sets are not being uses for unauthorised purposes to afford protection under the EU	States issue eMRTDs with ICAO/EU protocols that use various cryptographic techniques and biometric datasets (face, fingerprint and potentially iris). The protocols deployed by each state's passport issuing authority differs considerably, e.g. UK does not use EAC, Germany Uses SAC in its identity cards Romania uses EAC; however, all used Passive Authentication. It is important that the inspection systems behind ABC eGates process eMRTD and the associated data in a standard manner not only to achieve or to demonstrate a particular deployment capability but to provide some consistency and reassurance as to what to expect for both the Border Control operators and also the travelling public. The latter wants assurance that their private data is being protected in accordance with this standard.	A combination of Frontex, suppliers and border agencies/end-users, plus independent academics	Border Control Agencies as a minimum operating requirements for System Integrators to provide and comply with the standard for such Inspection Systems. It could also be used by Border Control Agencies in their tender documentation.	Consistency in automatically inspecting an eMRTD with the eMRTD holder. A holder and their eMRTD should achieve the same outcome irrespective of the border control crossing's ABC. Basically, the public's perception and also that of some Border Control Authorities that a certain degree of reliability can be placed on eMRTDs and eMRTD Inspection Systems.

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	Privacy Directive.				
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 2 Dilemma: Does this imply security functions or security of the ABC itself? In any case, both should be dealt with- as a set of requirements are needed. This is linked with B7 and B8. A combination of both was suggested. *Olivier Monsacre: For C11, I had a P1 as noted, not P2*.				
C12	Is there a need for guidance and/or rules for privacy protecting technical concepts within standardisation?	Lack of implementing Privacy by Design	CEN TC224 WG18	Industry	Better acceptance of security technologies by the public.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: No priority has been indicated. Similar to C5- To be combined.				
C13	It might be priority 1 but it depends on the outcome of the FRONTEX+ DG Home discussions. In general, all the systems need to be tested and all the test methods are to be validated and then standardized. There si a lot of hesitation on how to approach testing and ensure the integrity of the testing in view of acceptance of certificates. *FRONTEX: There are no such discussions … This was never implied during the Workshop.* *Olivier Monsacre: For C13, It was to be linked to C11.*				
C14	Priority; no score The same discussion was on subject A17. It is not a request for a standard but for a specification of a scheme. Some members of the group want to solve this issue. At this time there is the possibility of unauthorised access to more data than necessary. It is a relevant issue for discussions about article 6.				

D The End User

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
D1	To establish standards and parameters for competence development regarding biometrics embedded in automated border control systems	The competence profile of operators of ABC systems diverse from the profile of the border guard or immigration officer. Clear qualification standards, level determination and standardisation, needs to be established for operational action. Standardised training should be executed to get maximum results and focus on threshold and procedures.	Public educational institutes with strong support of suppliers and border agencies/end-users, plus independent academics.	Border guards, immigration officers, police forces and other governmental organisations responsible for ID authentication.	A standardised competence profiles, based on the latest technology and didactical methodology. Certification and establishing knowledge disclosure parameters. Bilateral and international exchange of information regarding biometrics and ABC technology
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score Chris summarizes this subject as 'a possible syllabus for bodyguards in ABC-systems'. This has to be a so called 'living' document. Relevant questions: • Do we require such a document? • Who is going to develop it? • How soon should we do this" FRONTEX is already developing first steps on this issue. E.g. scope of such training. There isn't one in the world at this moment. We mustn't forget follow-ups. *FRONTEX: Frontex is currently exploring in cooperation with the MSs the possibility to develop a training on vulnerability assessment of biometric systems with a specific focus on ABC*				
D2	Formation of technical group (and creation of a continually updated Technical Report) which looks ahead to future developments in ABC and associated requirements for standardisation. One example of this is remote stand-off /on the move biometrics capture, where recognition may be integrated with other security functionalities	Act as a forum for exchange of proposals and innovation in integrated border management systems, with a remit of encouraging early work on standards specific to such systems	CEN/Frontex?	Component and system suppliers. Authorities deploying and maintaining ABC systems	Standards will be available earlier, authorities will be aware in advance of new opportunities and be able to develop better roadmaps and strategies for border security. Support for the EU security sector in that innovative systems will be demonstrated to conform to standards.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	There are already an ABC-working group and ABC-workshops and a global ABC-conference, under the responsibility of FRONTEX. These groups should recognize the need for standards at an early time (it should be on the agenda constantly). *FRONTEX:* *This is a user-driven approach to harmonisation. Not the role of Frontex* *There are also other relevant international working groups under the umbrella of ICAO, IATA, ACI … For example, ACI and IATA are developing an implementation guide for ABC from the perspective of carriers and airport operators*				
D3	Define minimal size and constraints of automated border control unit (i.e. eGate) to comply with international requirements for reduce mobility people.	Ensure that no discrimination is performed and all standard equipment used by reduced mobility people are accepted.	Suppliers, border agencies, Frontex, ICAO, IATA, advisors on special needs, end users, academics.	Suppliers and purchasers	A published standard, compliance to which can be independently verified, which informs purchasers and managers of ABC systems of requirement for reduced mobility people.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score In several countries this issue is covered by legislation (probably European-wide). Some disabilities are rare. The question therefor is to what level do we want to go to? There is always the alternative of a manual gate! The group agrees that this is more a subject for a standard specification or a procedure.				
D4	Communication interface, data-format and command standardisation between ABC equipment (i.e. eGate) and managing system of ABC.	The management and back-office system of a running ABC shall not be dependent of a specific equipment provider. It is recommended to define standardised an interface between the equipment and the system. Therefore, when new equipment shall be deployed or if new provider can proposed a more effective solution, it is not mandatory to change the full system or pay for specific development.	Suppliers, border agencies, Frontex, IATA, advisors on special needs, end-users.	Suppliers and purchasers	A published standard, compliance to which can be independently verified, which informs purchasers and managers of ABC systems as the performance to be expected – and relied upon – from their products. It ensure interoperability of all equipment provider or system provider.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 1 This subject has also been discussed in group A. It is a priority for the EC but it is not easy to achieve. The group is reminded that ICT is out of the scope of our Mandate. Nevertheless, the group wants to give it a priority 1. As soon as this becomes known, the industry knows what is being expected of them in time.				

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	Olivier Monsacre: For D4, I do not agree with your comment, stating it is not easy to achieve. It exist for a lot of product in the world, why not eGate? And it is not ICT, but interface of a component (the eGate) and the back-office system controlling a set of eGates. It is similar as your Credit card communicating with a payment reader. The communication protocol and the information exchanged are standardised.-				
D5	Vocal guidance for reduced sight or blind travellers inside the gate, using language recognised by passport nationality	It shall offer the same service to disabled people not able to read written guidance and not familiar with the local language or English.	Suppliers, border agencies/end-users, plus blind service advisor.	Suppliers in building new systems; end users in specifying requirements for systems.	For people with reduced vision or blind, the use of an understandable language based will enable the use of gates by disabled people. In addition, it will also help other people as well such as foreigner first timer not very familiar with local language or English. It will reduce the amount of assistance and offer a better equity for all type of population.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 4 This seems to be a subject for ISO. We mustn't forget that this specific group of travellers is always accompanied by an assistant. And nowadays, 2 persons in the gate will cause an alarm! There is a connection with D3.				
D6	To establish standards and parameters for radiation level allowed	Passengers have the fear that the radiation absorbed by the eGates could harm their health	Suppliers and health authorities, plus independent academics	Suppliers and border agencies	A published standard, which compliance can be certified and made visible by a sticker etc.
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: no score There are stickers available for this issue. The group agrees that this is a subject for local health authorities.				
D7	Create a standard signage for eGates	Passengers are confused with diverging signage used in connection with eGates in the EU	Border agencies, Frontex, advisors, academics, end users	Border agencies, FRONTEX, airport operators	Beneficial – making systems much easier to use for both first-time and regular users; also to reduce the amount of assistance required from carrier and port staff.

Item	What is the proposal?	Why is it necessary?	Who will develop the standard?	Who will benefit?	Expected benefit?
	TECHNICAL STANDARDS AREA: Common performance standards for ABC ICAO 9303 RECOMMENDED PROCEDURE AREA: Common operational procedures ICAO/Frontex Operational Guidance PRIORITY: 1 See also subject B20. These two subjects have to be merged. *FRONTEX: Note that Frontex has created a model sign to denote the presence of an ABC system which is being used in some countries and also features in the Commission Smart Borders initiative*				

B.3 Overview of Automated Border Control (ABC)

Automated Border Control (ABC) is a phenomenon which has begun to appear in the world's airports, seaports and land border crossings more or less only within the last fifteen years. That it has emerged during *this* period is partly because of problems faced by border control authorities in managing ever-growing numbers of passengers and partly because the necessary technology was becoming more usable and cost-effective.

As a result of this emerging market, more technology companies have been making ABC products available.

Another major factor is the early agreement by most of the world's governments to embed biographic and biometric data into radio frequency identity devices (RFID) into their travel document according to *standards* formulated by the International Commercial Aviation Organisation (ICAO).

There are several other factors which have promoted ABC include political changes which have enlarged common travel areas (e.g. the enlargement of the European Union and its Schengen area - and *interoperability* between neighbouring countries such as Australia and New Zealand, the USA and Canada, Singapore and Malaysia, Hong Kong and the People's Republic of China). This has resulted in much larger numbers of passengers now subject to light-touch immigration control. For example, at some UK airports, as many as 95% of passengers are European Union nationals who merely have to establish their citizenship to be admitted. The majority of these can use ABC. Some neighbouring countries even have a cross-border 'tidal flow' of people moving daily from home to work and back again.

Financial and commercial pressures have also promoted a self-service approach to many business and administrative transactions and international travel is no exception. The rise in the numbers of travellers, together with pressure on government budgets has encouraged immigration authorities to trial ABC solutions. The traditional border guard's role is likely to remain for the foreseeable future, with additional responsibilities such as overseeing the operation of ABC gates and managing those travellers who have been rejected at the automated solutions. Business benefits are maximised by *interoperable* systems, much in the same way as electronic banking systems are common across many financial enterprises.

Apart from travel document commonality, ABC did not spring up with ready-made standard *procedures* or design *methodologies*. Only recently has there been a trend to consider these, as the benefits of a standardised and interoperable solution are recognised, rather than a proliferation of isolated solutions.

ABC systems can be put together by systems integrators from bought-in components from different specialist suppliers or purchased as commercial off-the-shelf (COTS) systems from a single supplier.

There is as yet neither compulsion on suppliers to meet technical standards nor on purchasers to follow recommended practices unless mandated by commercial contracts, organisational policy or legislation. A random review of supplier technical literature for ABC components shows some mention of standards (e.g. 'Features the acquisition and assessment of ISO 19794-5 compliant images').

Fortunately, there are no ‘technology wars’ of the *VHS vs. Betamax* or *Apple vs. Microsoft* type. Of the many biometric modalities, only face, fingerprint and iris pattern are generally accepted as valid for e-Passports and consequently border control. In the future, should function and performance be standardised, the opportunity for supplier differentiation will be in the design and configuration of the component parts of an ABC gate.

This is not to claim that the last few pieces of the standards jigsaw puzzle should not be found and inserted in the correct gaps. There are benefits for both customers and suppliers on a common understanding of what is required and what is available.

ISO’s SC37 (biometrics) work is continuing and ABC and other identity management applications are often used as examples or subjects of technical reporting.

CEN’s technical committee TC/224 (work group WG18) is currently working on technical specification (CEN/TS 16634) for biometric ABC systems, though a number of the issues discussed in this document are out of its scope:

“This TS primarily focuses on biometric aspects of Automated Border Control (ABC) systems. Drawing on the first European and international ABC deployments, it aims to disseminate best practice experiences with a view to ensure consistent security levels in European ABC deployments. Furthermore, the best practice recommendations given here shall help make border control authorities' processes more efficient, speeding up border clearance, and delivering an improved experience to travellers.

ISO/IEC has published a series of standards dealing with biometric data coding, interfaces, performance tests as well as compliance tests. In order to promote global interoperability it is essential that all these standards are applied in European deployments. However, these standards do not consider national or regional characteristics; in particular, they do not consider European Union privacy and data protection regulation as well as European accessibility and usability requirements [7]. Thus, this Technical Specification amends the ISO standards with respect to special European conditions and constraints.

The TS systematically discusses issues to be considered when planning and deploying biometric systems for ABC and gives best practice recommendations for those types of systems that are or will be in use in Europe. The document deals with personal identification including ergonomic aspects that have an impact on the acquisition of biometric data.

Communication, infrastructure scalability and security aspects other than those related to biometrics are not considered. This document also does not consider hardware and security requirements of biometric equipment and does not recommend general border crossing procedures.

The enrolment process, e. g. for electronic passports, is out of scope of this document.”

CEN also plans further work on environmental influence for operational deployments of European ABC systems and mobile ABC systems.

Annex C
(Informative)

Crisis management

C.1 Existing standards

There is a rather extensive standardization landscape in the field of ISO/TC 223 Societal Security, with published documents:

Document	Title:
ISO 22300 : 2012	Societal security – Terminology
ISO 22301 : 2012	**Societal security – Business continuity management systems – Requirements**
ISO 22311 : 2012	Societal security – Video surveillance – Export interoperability
ISO/TR 22312 : 2011	Societal security – Technological capabilities
ISO 22313 : 2012	Societal security – Business continuity management systems – Guidance
ISO 22320 : 2011	Societal security – Emergency management – Requirements for incident response
ISO/PAS 22399 : 2007	Societal security – Guideline for incident preparedness and operational continuity management

This ISO/TC is also developing several other documents:

Document	Title:
ISO 22315	**Societal security – Mass evacuation – Guidelines for planning**
ISO 22316	Societal security – Organizational resilience – Principles and guidelines
ISO 22322	**Societal security – Emergency management – Public warning systems**
ISO 22324	Societal security – Emergency management – Colour-coded alert
ISO 22325	Societal security – Emergency management – Capability assessment
ISO 22351/2	Societal security – Emergency management – Shared situation awareness
ISO 22397	Societal security – Guidelines for establishing partnering arrangements
ISO 22398	**Societal security – Guidelines for exercises**

Not only ISO/TC 223 is working in the field of Social Security. Also ISO/TC 8 (SC 11 in general) has developed several documents on this issue, which have been included:

Document	Title:
ISO 28000 : 2007	Specifications for Security management systems of the Supply Chain
ISO 28001 : 2007	**Security management systems of the Supply Chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance**

Document	Title:
ISO 28002 : DIS 2010	**Development of resilience in the supply chain – Requirements with guidance for use.**
ISO 28003 : 2007	Requirements for bodies supplying audit and certification of supply chain security management systems
ISO 28004 : 2007	Guidelines for the implementation of ISO 28000

together with CEN/TC 379 Supply chain security.

And information systems standards, mainly:

Document	Title:
ISO 27001 : 2005	Information technologies – Security techniques – Security management systems - Requirements
ISO 27002 : 2005	Information technologies – Security techniques – Code of practice for information security management
ISO 27005 : 2005	Information technologies – Security techniques – Information security risk management
ISO/IEC 27031 : 2011	**Information technologies – Security techniques – general guidelines for preparing information technologies for business continuity**

And all texts relating to risk management, with the two most important ones:

Document	Title
ISO guide 73: 2009	Risk management vocabulary
ISO 31000 : 2009	Risk management – Principles and guidelines

The last important area of standardization is ISO / TC211 concerning Geographic Information (and linkage with the Open Geospatial Consortium, OGC), and particularly:

- ISO / TS 19101-2 reference model
- ISO / TS 19115-2 meta data
- ISO / TS 19103 schema language
- ISO / TS 19104 terms needed

together with CEN/TC 287 on geographic information.

Other standardization domains are not listed here, because they are too far away from the mandate M/487, namely ITU and ETSI standards.

In addition there are national standards and technical specifications to consider:

Document	Title	State
BS 25999 part 1 : 2006	Business continuity management code of practice	UK
BS 25999 part 2 : 2007	Business continuity management specifications	UK
NFPA 1600 : 2010	Standard on Disaster/Emergency Management and Business Continuity Programs	USA +

Document	Title	State
ASIS SPC.1 : 2009	On Organizational Resilience, Management System Requirements	USA
DIN ASTM E 2641 V2010	Standard Guide for Resource Management in Emergency Management and Homeland Security	Germany
ZA SABS 264-1 2/3 2002	Disaster Management parts 1,2,3	South Africa
INS 24001 : 2007	Security and continuity management systems – Requirements and guidance for use	Israel

C.2 Workshop

Program workshop at Edinburgh

Workshop Agenda 09. April 2013		
13:00 – 13:30	Welcome and Introduction	Joost Cornet, Chair of M/487 coordination group Sue Ellen, General Director, City of Edinburgh Hans-Martin Pastuszka, EC DG Enterprise and Industry
13:30 – 14:00	Setting the Scene	Alain Coursaget, M/487 project expert for Crisis Management/Civil Protection
14:00 – 15:30	Workshops: Areas A&B	All Participants
15:30 – 16:00	Coffee Break	All Participants
16:00 – 16:30	Workshops Continued	All Participants
16:30 – 17:50	Presentations: Areas A&B	Moderators
17:50 – 18:00	Closure	Joost Cornet
Evening	Evening Activity	
10. April 2013		
09:00 – 10:30	Workshops : Areas C&D	All Participants
10:30 – 11:00	Coffee Break	All Participants
11:00 – 11:30	Workshops Continued	All Participants
11:30 – 12:50	Presentations: Areas C&D	Moderators
12:50 – 13:20	Q&A	Q&A for the coordination group M/487
13:20 – 13:30	Closure	Joost Cornet
13.30		Lunch

Main outcomes

Priority 1

Working Group number	Proposals numbers within WG	Description of the proposal
WG1 Emergency Response Planning and Resiliency		
WG1	 1 9	Principles: Basic emergency response principles to facilitate interoperability Linkage with risk register / risk analysis
WG1	 3 7	Semantic: Provide definition of risk manager, crisis, crisis room, emergency, resilience Generate a dictionary comprising at least the most important European languages in addition to the vocabulary list ISO 22300 to facilitate communication
WG1	 20 24	Planning methodology: Define “limited key information” to share (pre, during, post incident) to improve preparedness, coordination and debriefing (between different actors and different hierarchical levels) Develop methodologies for anticipation and decision making process under uncertainty (when there is a lack of information, unreliable situation assessment, uncertainty about situation evolution)
WG1	 38,39,40 41	Debrief: Define exercises evaluation procedures : Crisis Management performance parameters, identified gaps, communication/planning/implementations of findings, develop lessons learned data base, produce a common lessons identified process (identification, implementation, inclusion in SOP or training courses) Standard for pan-European after crisis handling *Comments: look at additions to ISO 22398 guidelines for exercises*
WG3 Incident management: first hour(s)		
WG3	 24,25,26	Warning (alert and notification) technical aspects : Standardization of technical aspects of alerting: • Develop client-based applications to decode alert messages in consumer receivers (smart phone, tablet, etc.) • Specify use of navigation enabled devices for alerting. • Establish a standard way to refer to administrative areas with geo-codes that are valid all over Europe for alerting purposes. *Comments: consider ISO 22324 “colour-coded alert”*
WG5 / C&C interoperability (Part 1, organisational interoperability)		
WG5	 1, 3,9	Organizational interoperability : To develop C&C interoperability model : establish a generic description of missions, responsibilities, functions, structure, for the different hierarchical layers, together with semantic model and interfaces with the outside world (general public, NGOs), in order to facilitate mapping of organizations within MS and between MS, to facilitate direct contacts at the right levels, in order to know the people, exchange liaison officers, identify the types of

Working Group number	Proposals numbers within WG	Description of the proposal
		information to exchange and facilitate coordination in a cross-border, cross-sector, multi-level, multi-hierarchy, public and private command situation, for coordination of situation assessment, response and communication to the public. Priority will be given to top layers communication needs. *Comments: preliminary work is needed, including capitalizing on existing work (i.e. Acrimas Project)*
WG6 / C&C interoperability (Part 2, communication interoperability)		
WG6	1 to 9	Structure of geospatial information : Develop standardized common geospatial basic information (based on existing GIS standards) to be used by organizations before and during crisis situations (for these organizations to provide additional information to the common base or to retrieve information to be consolidated within their own systems). This common geospatial basic information should use minimum semantic agreements and minimum standardized Icons. It could also include geospatial information for underground facilities and buildings. It would eventually evolve later towards a more developed meta data reference.

Priority 2

Working Group number	Proposals numbers within WG	Description of the proposal
WG1 Emergency Response Planning and Resiliency		
WG1	2 8	Semantic: Executive level overall presentation and clarification of relationship between management systems: risk management / crisis management / activity continuity / resiliency. To facilitate communication by ensuring semantic interoperability of map objects (icons and terms) between Emergency Management Systems (EMS) by providing mappings among different classifications at both national and international level (see C&C interoperability).
WG1	34,36	Resiliency: We need a resiliency standard about good practice & concept for crisis management based on agility, more than on planning. This standard will improve territorial resiliency (first hour quick actions to undertake, fall back mode). It concerns both agility during response phase and preparation for agility. It assumes a good understanding of context (organisation and capabilities).
WG2 Preparedness		
WG2	1,2,4,7 8,9,11	Awareness: Reinforce citizen and local territorial community awareness and involvement. Increase knowledge of risks and available channels for information and advice for appropriate actions (before, during and after the incident). Warning (alert and notification) dissemination understanding. Develop alert libraries that are applicable in all European countries. Define common European messages schemes for fire and evacuation systems. *Comments: use ISO 22322 "Public warning" defined process.*
WG3 Incident management: first hour(s)		
WG3	4	Detection: Qualification, escalation process and warning decision process

Working Group number	Proposals numbers within WG	Description of the proposal
WG3	5,7,8, 10	Reporting: Standardize the way of acquiring digital information from victims/public and sending it to the whole command & control system (it may include developing a common 'victim ticket', to be filled in by victims using smart phone emergency applications). *More research needed: look at current FP7 projects for more concrete ideas, such as the use of smart-phones/tablets and new standards for emergency calls using VoIP and advanced caller location identification. Consider issues such as the protection of personal information or the impact of national legislation or the saturation of the public safety answering point (PSAP).*
WG3	22 23 + WG 4-2	Warning (alert and notification) common language: Develop alert libraries that are applicable in all European countries. Develop a communication protocol that allows lightweight transmission of alert messages and supports light encoding of the alert libraries, with possible use of wireless media (suggest more specific use of CAP, based on alert libraries, to allow interoperability) *Comment: basic idea is on having standard alert message format independent on the channel being used. Two elements: (1) alert messages should be structured in the same way everywhere (2) with the use of a standard library/ a common language for all languages. The currently existing CAP is not covering this all, but just provides a structure. Check the FP7 project PEPPOL (on interoperability of government services).*
WG4 Operational efficiency		
WG4	1,3 5 6	First responder communication : *Comment: this has to be further analysed. Look at FP7 ISITEP project to establish a EU network where forces share (cross border) communications. On the technical side, standardization is managed in 3GPP and TCCA working groups, in close coordination with ETSI. This topic is therefore deleted from the list of proposed standardization for CEN, and could remain a subject for further research on the usage side.* Facilitate radio communication interoperability (voice, data, image) To develop standards for the usage of mobile broadband services in addition to the professional mobile radio PMR. This shall improve the information exchange of emergency management organisations (e.g. based on LTE, WIFI, whatsoever) Develop an easy and standardized way to link arbitrary smart phones together in order to exchange incident-relevant data
WG4	11 WG3-40	Assistance to first responders (localisation) : Geo-localization (GIS) standards for use in buildings and underground systems to facilitate FR intervention Standardization for providing dynamic information during an emergency (i.e. evacuation information in real time, location, infrastructure availability, exit routes availability)
WG4	13 WG3-6	Emergency management interoperability : Standardization of detection equipment for search and recue (to facilitate international missions). Distress beacon app. for smart phones to be activated by victim.
WG4	17, 18	Assistance for victims management : Standards on patient-management in mass casualty incidents (e.g. minimal data-set for patient-management in mass casualty incidents, management of data of affected persons in mass casualties,…). To close the gap in (inter)national pre-hospital patient-management with differing national standards. Develop a standardized electronic triage system to improve the logistics and the situation awareness.
WG4	12	First responder tools: Facilitate indoor localisation using radio wireless communication protocols (to be linked with proposal 11)

Working Group number	Proposals numbers within WG	Description of the proposal
	14	Facilitate interoperability of unmanned search and rescue equipment *<u>Comment:</u> this proposal need to be further analysed and could move to P4*
WG6 / C&C interoperability (Part 2, communication interoperability)		
WG6	10 to 18	C&C communication interoperability : Develop communication interoperability by a better definition of needs and the use of minimum common semantic and minimum set of requirements. It will be implemented on a volunteer basis, considering existing implementations (i.e. in the Netherlands with information architecture for security, in Austria and in FP7 CRISMA project). This work will eventually allow progressive standardization of event description and of digital objects, adaptation to evolving technologies and facilitate mechanisms to share information on a day-by-day basis.

Priority 3

Working Group number	Proposals numbers within WG	Description of the proposal
WG2 Preparedness		
WG2	17,18,19	Training: Training on how to run simple exercises (plan, execute and report). Involve citizen, communities and organisations with plans to increase community resilience. Pan-European collective training (table-top, simulation, operational). Multi-agency, common cross-border training program (share best practices, networking, get to know each other, continuous improvement) *<u>Comments</u> : check developments from ISO 22398 (guidelines for exercises)*

Priority 4

Working Group number	Proposals numbers within WG	Description of the proposal
WG1 Emergency Response Planning and Resiliency		
WG1	 10 11	Planning methodology: EU harmonized risk/impact assessment and evaluation of risk acceptance methodologies. To support capacity building on a structured risk assessment & a set of minimal capability requirement

Best practices (to be continued)

Working Group number	Proposals numbers within WG	Description of the proposal
WG3 Incident management: first hour(s)		
WG3	1 2	Use of social media Early detection through weak signals *Comments: This topic could easily evolved towards a standard on how to best detect, qualify and exchange(sometimes classified) information about early signals at a European level*
WG3	31	Methodology for sourcing information (social media, tweets, crowd source information) to assess impact of wide scale disaster and identify public needs
WG3	36	Develop smart phone emergency specific applications (situation reporting, CCTV capabilities, citizen as a sensor, etc.)
WG3	41	Develop a common and standardized procedure in order to let citizens actively bring in their resources into the relieve effort (e.g. a 'resource ticket' available on mobile phones and the web)
WG5 / C&C interoperability (Part 1, organisational interoperability)		
WG5	2,4,5,6,9, 10	Best practices in application of the generic organisational model (proposal WG5-1): - differentiate the vertical layers and clarify semantic - develop coordination at the strategic level for complex cross-sector major crisis - develop procedures for collaboration - close interoperability gaps in international crisis and disaster response - roles and responsibilities are clearly identified prior to any crisis - clearer understanding of deliverables before, during and after the crisis - deliver a set of common 'Business Protocols' across the area of communication
WG5	26	Creation of a centralized data base of events, decisions, following actions plans for memorizing all important information with their date, hour

Further analysis required

Working Group number	Proposals numbers within WG	Description of the proposal
WG2 Preparedness (simulation tools, training)		
WG2	14,15	Standardization of objects models (digital re-usable assets) for modelling and simulation environment (application for cross-boundary training). Standardization for building information with object models for the representation of both structural and functional aspects of facilities. It is useful for simulation of service deployment for transport system and for rescue personnel training. *Comment: look at interrupted work ISO 22351/52 on shared situation awareness*
WG4/ Operational efficiency		
WG4	15	Development of standards based on bottom-up identification of the minimum improvements expected hands-on by field staff (electrical plugs for generators, diameter of pipes, etc.)

Working Group number	**Proposals numbers within WG**	**Description of the proposal**
WG5 / C&C interoperability (Part 1, organisational interoperability)		
WG5	11, 12	Improve the management of vertical bottom-up information flow for situation assessment, both within the public sector and within private organizations to facilitate and accelerate real understanding of key issues, critical information, priorities and to develop capacity to anticipate situation evolution by a better understanding of next layer expectations. Improve decision support system and situation awareness by information filtering & delivery for top level organisations
WG5	19	To define standardised sets of meta-data for risk descriptions including co-ordinates, probability, severity, nature of the risk and possible triggers *Comments: it should be a long term priority*
WG6 / C&C interoperability (Part 2, communication interoperability)		
WG6	19	Facilitate information exchange between Crisis Management/Civil Protection and Critical National Infrastructure Operators

Annex D
(Informative)

CBRNE

D.1 Existing standards

Document	Title	State
SEC (2010) 1626 Final	Commission Staff Working Document Risk Assessment and Mapping Guidelines for Disaster management.	EU – Civil protection Mechanism
SWD (2012) 169 Final	Commission Staff Working Document EU Host Nation Support Guidelines	EU – Civil protection Mechanism
2010/418/EU, Euratom	COMMISSION DECISION of 29 July 2010 amending Decision 2004/277/EC, Euratom as regards rules for the implementation of Council Decision 2007/779/EC, Euratom establishing a Community civil protection mechanism General requirements for European civil protection modules.	EU – Civil protection Mechanism
Ares (2013) 1790026 – 06/06/2013	Guidelines for Standard Operating Procedures (SOP) Fo0r Civil Protection Modules	EU – Civil protection Mechanism
CEN/TS 16595:2013 (Draft)	CBRN - Vulnerability Assessment and Protection of People at Risk	
Glossary on CBRN http://www.nucleonica.com/CBRN/	An Information Tool for Practitioners in Protection and Response	European Union

D.2 Workshop

Program workshop at Ispra

Workshop Agenda 11. April 2013		
13:00 – 13:30	Welcome and Introduction	Joost Cornet, Chair of M/487 coordination group Naouma Kourti JRC Ispra Hans-Martin Pastuszka, EC DG Enterprise and Industry
13:30 – 14:00	Setting the Scene	Eelco Dijkstra, M/487 project expert for CBRNE
14:00 – 15:30	Workshops: Areas A&B	All Participants
15:30 – 16:00	Coffee Break	All Participants
16:00 – 16:30	Workshops Continued	All Participants
16:30 – 17:50	Presentations: Areas A&B	Moderators
17:50 – 18:00	Closure	Joost Cornet
Evening	Evening Activity	
12. April 2013		
09:00 – 10:30	Workshops : Areas C&D	All Participants
10:30 – 11:00	Coffee Break	All Participants
11:00 – 11:30	Workshops Continued	All Participants
11:30 – 12:50	Presentations: Areas C&D	Moderators
12:50 – 13:20	Q&A	Q&A for the coordination group M/487
13:20 – 13:30	Closure	Joost Cornet
13.30		Lunch

In the following tables a detailed description of the results of the workshop on CBRNE is included. After each Proposal the number of groups that discussed the proposal (including the chosen priority) is shown.

M/487 EUROPEAN STANDARDISATION ROADMAP FOR CBRNE: PROPOSALS

Code	What is the proposal?	G1	G2	G3	G4	G5	G6	Suggestions for follow up:
A1- 1	To develop standards for level of detection for biological, chemical radiological and industrial (TIC'S) devices	3		4	2		1	
A1-2	To develop standards for biodetection devices		4	4	2	2 or 1	2	
	To develop standards for			4	2		2	
	Standard for personal mini "Bio-detector" and identifier		3	3		4	2	
A2-3	Standard for "First Responder CBRE and low Oxygen level warning instrument" ("PWARN" a FR (personal) detector including CBREO sub detectors to warn the FR in defined levels of contamination (mini)	1	2	2		1	2	
A4 -1	To develop standards for installation proper and easy detection equipment in public places	4	2	3	1		2	
A4-2	To develop standards (protective measures) to protect people in public buildings against toxic effect of possibly leaking chemicals	4	2	1	1		2	
A4-3	To develop standards for general ventilation protective air filtration solutions	3	2	4	1	1 /3	2	
A4-4	To develop standards which regulate under which boundary conditions a built critical infrastructure has to consider an explosive threat and which verifications are needed to prove the sufficient resistance against this threat.	2	2	2			1	

A5-1	To develop standards for the systematic radiation detection of checked baggage or air cargo.	1	3	1			1	
A5-2	To develop standards for the systematic radiation scanning of on board baggage and passengers.	1	3	1			1	
A5-3	To develop standards for Explosive Trace Detection equipment (ETD), used in Aviation Security (AVSEC)	1		1	1		1	
	To develop Standard Test Piece (STP) for Liquids Explosive Detection Systems (LEDS) equipments	2		2				
A6-1	To standardize the definition of “water quality”, required responses and validation of these techniques	1		1		2/4	2	
A6-2	To create standards of **online** monitoring techniques	1		2	1	2/4	2	
A6-3	to develop standards for **real-time** measurements for pathogenic organisms			2	1	2/4	2	
A6-4	To develop standards for **real-time** measurements for toxic substances	4			1	2/4	2	
A6-5	Develop standards for radionuclides detection			2	1	2/4	1	
A7-1	Minimum detection standards for explosives detection devices outside the area of aviation security	1	2	3	1	3	1	
A7-2	To develop standards for bulk detection	2	2	1	3	4	2	

A7-3	To develop standards for trace detection	2	2	1	1	1	2	
A7-4	To develop standards for standoff detection	2	2		2	4	2	
A8	To develop one standard for critical values / critical levels of hazardous materials in **- air** **- human being bodies**	3			1	3	CRN1 B2	
A9	To develop standards for emergency					2/4	4	
A10-1	Standard(s) for displaying building-premises information and capabilities (cars, equipment and personal) in GIS-systems.	4		3		1	3	
A10-2	Standard(s) for displaying the location of CBRNE substances (type, quantity and dangerousness) in GIS-systems. - Should be a CBRNE specific enhancement of a general GIS-standards	2		3		1	1	
B1-1	Standard guide lines and check list for CBR+ sampling by FR	1	1	3	2	1		
B1-2	Standard Sampling kit for CBR+ Sampling for FR	1	1	3	2	1		
	To develop standards for handling environmental samples (gases, fluids, solids) in dangerous conditions (C or B contamination) using mobile robot equipped with remote samplers	4	1	2				
	To develop standards for remote controlled radiation measurements and sampling using unmanned vehicles	2	1	2				
B2-1	To develop standards for list-mode data acquisition based on digital electronics	1		1	1	1		

B2-2	To develop standards for list-mode data acquisition based on digital electronics	2		1	1	1		
	To develop standards for expert support of field teams	1		1		1		
	Standard guidelines for Psychosocial Crisis Management in CBRNE Incidents							
B5-1	To develop standards for Full Facepiece Air Purifying **Respirators** (APR)	1	1		1	1		
B5-2	To develop standards for **Personal Protective Clothing (PPC**) (including gloves and footwear) used to Protect Against from Chemical, Biological, Radiological, and Nuclear (CBRN) Agents	1	1		1	1		
	To develop standards for	4	4					
	To develop advanced standards and strategies/doctrines for fast response in naval/maritime environment, border protection and the new asymmetric threats, maritime search & rescue operations							
	(c) Validation of age-dependent dose calculation methodology for critical groups	3		3	4			
	Standard for “Life Saving Decontamination” on the border of “Hot and Warm Zone”	1	2					
	To standardise and integrate rules for handheld sampling and detection procedures among EU and world organisations (OPCW, NATO, etc.)	3		4			2	
	To integrate standards for handheld sampling and detection devices in case of leaking chemicals	2		4			3	
	To develop standards for data base of biological, chemical , radiological and industrial devices			2				

D4-1	To develop an EU accepted list of standard reference materials for CBRNE agents in various type of samples	2	1	4	Trace 1 Bulk 2		1	
D4-2	To develop standard reference materials for the missing CBRNE agents in various type of samples (see above)	2	2			1	2	
D-5	To develop standards for the evaluation of **biodetection** devices	2	1 (A1-3)		4		2	
D-6	To develop standards for the evaluation of the efficacy of **decontamination** devices & protocols	2	1 (A1-4)	2	3	1	2	
	To develop new standards providing technical and functional requirements for handheld	3	2 (A1-5)					
	Standard for “Planning Guidelines” for First Response in a CBRNE incident (resulting in a common joint local “Incident plan”)	4				1	3	
D-9	To develop CBRNE Sampling and Detection **standard operating procedures** (SOPs) at strategic, operational, and tactical levels to enable preparedness and response for CBRNE incidents.	3		2	4		2	
D-11	To develop standard **testing and evaluation (T&E) methodologies** to assess the performance of CBRNE Sampling and Detection equipment	2	2	2	2	1/2	2	
D-12	To develop standards for **CBRNE Laboratory Analytical Methods**	2	4	2	See SLAM		2	
D13-1	Develop EU-wide explosive detection standards and testing methodology for trace particle and vapour based threats	1 / 2	2	2	2	1	?	
	Determine the							

	Assign rationale for adopting threat levels for explosive standards of			4				
	To develop harmonized methods and procedures to test CBRN protective equipment; more in particular to perform testing and evaluation of chemical and biological detection and identification equipment	1			Merge with B5	1		
	Standards to include	2	2 (GL)	2				
	While safety food standard is fully established, the security standard in the area of			2 (research)	?	2		
	To unify protective action distances useful to protect people	1				2		
	To further develop standardization in the field of biological toxins of potential bioterrorism risk; this important field has just been initiated in the course of the EQuATox project	2	2	2				
D-21	To recommend professional literature source/database/simulation software programme for chemical accidents, on line versions (ERG, Wiser etc.)							OUT
	Standards to certify security personnel			2 (D10)	1			
	To discuss options on how the ESO can contribute to an				2			
D23	Standard(s) for sensors and sensor dat**a** The idea is that new sensors will become more like computer components; and because they conform to standards they can therefore easier, faster and cheaper being integrated in operational sensor units or systems.	2		2	2	2	1-2	
D-24	To develop **common interoperability standards** between CBRNE detection and sampling equipment and end-users, and between networked devices and systems for CBRNE detection and sampling equipment for the capture, processing, and communication of data, as well as the display and reporting of results to end-users and decision makers.	2	2	1 (B3)	2	2	1-2	

D.3 Stakeholderanalysis CBRNE

Stakeholder 1: MANUFACTURERS/SUPPLIERS IN CBRNE DETECTION

GLOBAL

Most of the major international manufacturers and suppliers of products[4], processes and systems tailor their activities and technologies to different markets and marketing segments which often coincide with different sectors of the Critical Infrastructure (CI), e.g. health, transport, ICT, energy, food, water, etc.

When specifically looking at 'SAMPLING AND DETECTION' of threats related to CBRNE, this tailoring of marketing segments often involves:

- **Transportation security.** X-ray systems used in the search for illegal and dangerous items; body scanning systems using technology to check for hidden threats; explosives detection screening in threat detection equipment for checked baggage, hand-baggage or air cargo.
- **Critical infrastructure security.** Sensors and threat detection equipment to safeguard vital installations and essential services.
- **Ports & Borders screening systems.** High energy X-ray systems equip customs officers with the technology for contraband detection and cargo manifest verification, as well as for greater security.
- **Military force protection.** Threat detection equipment to identify chemical and biological warfare agents.
- **Emergency responders.** Equipping first responders and law enforcement officers with threat detection equipment, for personal protection or surveys, and rugged, portable products to identify unknown substances.

EUROPE

IMG-S

Other than the information on manufacturers and suppliers in Europe that can be obtained from EC sources (i.e. DG ENTR and DG HOME), an interesting network exists: the **Integrated Mission Group for Security**, IMG-S. It is an open forum which brings together technology experts from Industry, SMEs, Research and Technology Organisations (RTOs) and Academia. Around 21 nations and 230 participants are represented. IMG-S has a Technical Area 6 (TA-6) on CBRNE.

http://www.imgs-eu.org

[4]

Industry (global)	Markets (global)
Smiths Detection	(air transportation, ports and borders, critical infrastructure and military)
Morpho	(air transportation),
Rapiscan	(air transportation, ports and borders, critical infrastructure),
L3 Security & Detection Systems	(air transportation),
Nuctech	(ports and borders),
AS&E	(ports and borders),
FLIR	(air transportation, defence),
SAIC	(ports and borders),
Chemring	(military),
Bruker	(military, emergency responders)
Thermo Fisher	(military, emergency responders)

EOS

As of 2013, the **European Organisation for Security** (EOS) represents the interests and expertise of 42 Members involved in Security providing technology Solutions and Services from 13 different countries of the European Economic Area, representing more than 65% of the European Security Market and 2 million employees in Europe.

EOS facilitates the coherent development of the European Security Market, supporting the widespread deployment and implementation of solutions and services to provide security and safety to citizens, governments and economy.

The absence of an EU-wide scheme for standardisation and the certification of security equipment has been a major cause for the fragmentation of the European Security market which hampers investments, efficiency, and which de facto slows down the EU's ability to respond and adapt quickly to new and emerging threats. This absence also hinders interoperability as a major driver for the harmonization of the European Security market.

In recognition of this fact, EOS has set up a Task Force on Standards and Certification back in 2009 when it started to work on defining a roadmap and taking stock of existing standards. EOS has received official liaison status with CEN/CENELEC - the European Committee for Standardization where it contributes to the Technical Committees on "Societal and Citizen Security" and "Supply Chain Security". Recently it has also been invited by the European Commission to support CEN's work as the main representative of the private sector in defining a roadmap and priorities for the development of security standards in fulfilment of DG ENTR's Programming Mandate on Security Standardization.

http://www.eos-eu.com/?Page=home

Industry forecast

Sources from within the industry offered in 2012 the following outlook:

"The demand for detection equipment, particularly in the large markets such as transportation, ports and borders and critical infrastructure (estimated at more than £1.6bn) is forecast to continue to grow at almost 7% per annum in the near-term because of ongoing geo-political unrest and the terrorist and criminal threats it creates.

The changing nature of the detection business sector is resulting in a growing volume of smaller contracts and fewer major programmes. It is also placing more emphasis on aftermarket sales, enhancing the level of customer service to meet opportunities arising from the extensive installed base of detection equipment across most regional markets.

The heavily regulated transportation sector is a large market; rising passenger volumes are resulting in new airport investment, especially in the Middle East and South East Asia. This, together with continuing security threats, a strong replacement cycle and globalisation of trade, boosting freight volumes, is expected to continue to support market growth. In addition more stringent requirements from major regulatory bodies will increase the sophistication of security equipment.

In the ports and borders market, demand for detection equipment is expected to rise to address a variety of threats as governments become increasingly concerned about cross-border security involving the smuggling of explosives, weapons and radiological materials, while continuing to recognise the strong revenue-generating potential from contraband detection."

- Overall demand in the highly fragmented critical infrastructure market continues to grow strongly. Governments and other organisations are seeking to protect their assets within current terror threat levels and increasing levels of perceived risk.

Stakeholder 2: STANDARDS DEVELOPMENT ORGANIZATIONS (SDO) - CBRNE

CEN - The European Committee for Standardization (CEN) is one of the three European Standardization Organisations (ESOs).

ISO - International Organization for Standardization is the world's largest developer and publisher of International Standards other than electro-technical or telecommunication ones. ISO is a network of the national standards institutes of 162 countries, based in Geneva.

IEC - The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electro-technical committees (IEC National Committees).

IEEE - Pronounced "Eye-triple-E," stands for the Institute of Electrical and Electronics Engineers and cites that it “creates an environment where members collaborate on world-changing technologies – from computing and sustainable energy systems, to aerospace, communications, robotics, healthcare, and more.”

Aviation Security - ECAC
In 2008 the 44 European Member States of the European Civil Aviation Conference (ECAC) developed technical specifications and Common Testing Methodologies as the basis for the implementation of its Common Evaluation Process of security equipment (CEP).
The CEP currently applies to Explosive Detection Systems (EDS), Liquid Explosive Detection Systems (LEDS) and Security Scanners. More than sixty equipment types have been evaluated to date. Under this scheme, participating test centres made available by national authorities in ECAC Member States evaluate the performance of EDS, LEDS and SSc and the results of these evaluations are transmitted to the ECAC Member States.
Authorities in charge of civil aviation security in each of the 44 Member States retain the prerogative of approving or certifying equipment for deployment at airports on their national territory. States may select equipment which they feel corresponds to national threat assessments or to the operational needs of their airports, while simultaneously meeting European requirements.
For further information on ECAC – CEP system: www.ecac-ceac.org

Stakeholder 3: GOVERNMENT/REGULATORY AGENCIES

EC – The EU’s next seven year general R&D budget (2014-2020) – known as Horizon 2020 – is now in its early preparatory phase. Part of it will be dedicated to security-oriented R&D.
In terms of CBRNE related activities the Council of the EU emphasizes that it is primarily Member States’ responsibility to protect the population against CBRNE incidents, be they of accidental, natural or intentional origin, and that initiatives at the EU level should be taken in accordance with the principles of subsidiarity and proportionality, as well as be guided by the principle of solidarity.
Please note that when one searches the EU CORDIS database of ‘security’ related projects from FP7 and before, the result is 2456 projects.

OPCW - The Organisation for the Prohibition of Chemical Weapons is the implementing body of the Chemical Weapons Convention (CWC), which entered into force in 1997. As of today the OPCW has 188 Member States, who are working together to achieve a world free from chemical weapons. They share the collective goal of preventing chemistry from ever again being used for warfare, thereby strengthening international security.
The OPCW Member States represent about 98% of the global population and landmass, as well as 98% of the worldwide chemical industry.
OPCW is currently re-examining an extension and a broadening of its mandate which may include CBRNE detection and security related activity.

WHO - The Expert Committee on Biological Standardization (ECBS) is commissioned by WHO to establish detailed recommendations and guidelines for the manufacturing, licensing, and control of blood products, cell regulators, vaccines and related in vitro diagnostic tests. Members of the Expert Committee are scientists from national control agencies, academia, research institutes, public health bodies and the pharmaceutical industry acting as individual experts and not as representatives of their respective organizations or employers. The decisions and recommendations of the Committee are based entirely on scientific principles and considerations of public health.
The Expert Committee on Biological Standardization meets on an annual basis since 1947 and is responsible for the establishment of the WHO International Biological Reference Preparations and for the adoption of the WHO Recommendations and Guidelines. The Expert Committee directly reports to the Executive Board, which is the executive arm of the World Health Assembly.

IAEA - The IAEA is the world's centre of cooperation in the nuclear field. It was set up in 1957 within the United Nations family. The Agency works with its Member States and multiple partners worldwide to promote safe, secure and peaceful nuclear technologies.
Safety standards and security guidance are continuously developed and updated in four technical areas:

- Incidents and Emergencies
- Nuclear Installations (Safety)
- Radiation, Transport and Waste
- Nuclear Security

The IAEA’s standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. Information on the IAEA’s safety standards programme (including editions in languages other than English) is available at the IAEA Internet site www-ns.iaea.org/standards/

Stakeholder 4: R&D / TESTING LABORATORIES

DG HOME– ERNCIP
As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle. Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.
The Institute for the Protection and Security of the Citizen (IPSC) is one of the seven institutes of the European Commission's Joint Research Centre (JRC).

Located in Ispra, Italy, the Institute provides scientific and technological support to European Union policies in different areas, including global stability and security, crisis management, maritime and fisheries policies and the protection of critical infrastructures. Moreover, the Institute performs statistics and information analysis for the evaluation of the effectiveness of policies and to enhance financial stability. IPSC works in close collaboration with research centres, universities, private companies and international organisations in a concerted effort to develop research-based solutions for the security and protection of citizens.

The **European Reference Network for Critical Infrastructure Protection (ERNCIP)** was set up by the IPSC to provide a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonize test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards. Their mission is to foster the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities. ERNCIP is a direct response to the lack of harmonised EU-wide testing or certification for CIP products and services, which is a barrier to future development and market acceptance of security solutions.

The mission of the **Security Technology Assessment Unit** is to increase European competitiveness by research towards the standardization and harmonisation of the protection of European networked infrastructures and hazardous industrial installations.

http://ipsc.jrc.ec.europa.eu/?id=688

Of particular relevance are the thematic areas that closely align with the M/487 CBRNE project. See http://ipsc.jrc.ec.europa.eu/index.php/Membership/776/0/.

Stakeholder 5: MILITARY

EDA

The European Defence Agency (EDA) supports the Council and the Member States in their effort to improve the European Union's defence capabilities for the Common Security and Defence Policy (CSDP).

This means running and supporting cooperative European defence projects; supporting research and technology development; boosting the European defence technological and industrial base; and providing a forum for European Ministries of Defence. It offers multinational solutions for capability improvement in a time where defence budget constraints foster the need for cooperation.

NATO

NATO publishes standardization agreements (STANAG) that establish common equipment requirements, military methods and technical procedures for all the NATO member states. Once adopted, a STANAG permits all members to operate and communicate efficiently with each other.

NATO STANAGs are used by defense international contractors, operating in the following defense-related industries: aerospace, electronics, engineering, computers and telecommunications.

The service has direct applications in research, design engineering, maintenance, purchasing, bidding, logistics and related applications.

The IHS NATO document service includes PDF images of the following unclassified NATO documents:

- NATO standardization agreements
- Allied Quality Assurance Publications (AQAPs)
- Miscellaneous standardization documents

Stakeholder 6: PROCURERS/USERS

PSO – Public Safety Organizations
This term is used to describe a wide variety of organisations and capacities by countries, states, cities, and regions to prevent and protect from events that could endanger the safety of the general public from significant danger, injury or harm, or damage.

FR – First responders
Particularly in the USA, this term has become very popular to describe volunteer and professional emergency personnel in areas such as EMS (emergency medical services), Explosives, Fire, HazMat (hazardous materials), Law Enforcement, and Search and Rescue.

In terms of standardization, a resource knowledge base exists in the USA specifically designed for FR to provide “emergency responders, purchasers, and planners with a trusted, integrated, online source of information on products, standards, certifications, grants, and other equipment-related information."
www.rkb.usa