

D1.2 Lessons identified and learned from past Programming Initiatives



Report Title:	D1.2 Lessons identified and learned from past Programming Initiatives
Author(s):	Jolien van Zetten, Ying Ying Lau, Christopher Liedtke, René Lindner, Else-Marie Fykse, Hans-Martin Pastuszka
Responsible Project Partner:	NEN

Document data:	File name (QMS compliant):	ResiStand_D1 2_v1 0_final.docx		
	Pages:	62	No. of annexes:	2
	Status:	Final	Dissemination level:	PU
Project title:	ResiStand: Increasing disaster Resilience by establishing a sustainable process to support Standardisation of technologies and services		GA No.:	700389
			Project No.:	12134
WP title:	WP1 Establishing the project's building blocks		Deliverable No:	D1.2
Date:	Due date:	August 31, 2016	Submission date:	August 26, 2016
	Keywords: Programming Initiative; Programming Mandates; processes; methodologies; review			
Reviewed by:	Michael Löscher,		Review date:	August 18, 2016
	Antti Karppinen		Review date:	August 18, 2016
Approved by Coordinator (GEO):	Pertti Woitsch		Approval date:	August 26, 2016

Delft, 26 August 2016



Project Contact

GEOWISE GEOWISE Oy, Mr. Pertti Woitsch, Rälssitie 7 A, 01510 Vantaa, Finland

ResiStand Project

Standardisation is a powerful tool to achieve better interoperability. However, it needs to overcome a lack of interest and modest participation from stakeholders. Also, promising research results are not always used as the basis for new standards.

The overall goal of ResiStand is to find new ways to improve the crisis management and disaster resilience capabilities of the European Union and individual Member States through standardisation.

ResiStand contributes to an improved disaster resilience by identifying and analysing the drivers, constraints and expectations of three main stakeholder communities: Standardisation Organisations, End-Users and Suppliers, consisting of researchers, industry and SMEs.

Based on this information, gaps in standardisation are identified and a prioritised roadmap for new initiatives will be created. The roadmap will be complemented by a critical evaluation of standards as a tool to improve disaster resilience.

ResiStand aims at implementing a pre-standardisation process that supports the development of standards. The feasibility of the process will be tested by developing a new work item. The aim is that stakeholders will continuously utilize this “ResiStand Process” in the future, and that the project delivers a better understanding of the potential of standards for contributing to an improved disaster resilience.

ResiStand will support the management of increasing threats to society such as armed conflicts, terrorism, pandemics and natural disasters, which have increasingly cross-border, even global consequences due to the on-going globalisation.

Protection of citizens through anticipation, preparedness, response and adaptation to crisis situations – i.e. maintaining disaster resilience – will be more efficient. Collaboration between national, European and international stakeholders will be improved by unified processes and management systems as well as by technical, procedural, operational and semantic interoperability.

Executive Summary

Most commonly, standards are initiated and developed by stakeholders participating in standardisation committees, while the process is facilitated by a standards body. In contrast to this bottom-up approach, the development of standards can also be requested by authorities through Programming Initiatives, a so-called top-down approach. This deliverable (D1.2) focuses on this top-down approach, and presents a review and analysis of the processes and methodologies of past Programming Initiatives.

A **Programming Initiative** (PI) is considered to be a request from an authority to one or multiple organisations or persons, to investigate which standards should or could be developed in the future to bring solutions for current technical and non-technical challenges. PIs can be issued by all types of authorities, being international, European, or national.

On national and international level, some PIs have been identified, including military PIs. However, the number of relevant PIs were limited, except on European level. Therefore these PIs will be first discussed before going into the study of the European PIs.

A **national** PI on electric mobility (Germany) was included, showing a good practice of a platform initiated by the German government to encourage information exchange between stakeholders and to develop a work programme for electric mobility, including related standardisation activities. Additionally the government also funded a project for setting up a standardisation framework. On **international** level, the 'Sendai Framework for Risk Reduction' in the UN framework was identified; even though standardisation is considered as an important and effective measure, no specific standardisation initiatives were identified.

Next to the civil PIs, also the **military** PIs have been analysed. The defence sector uses either civil, dual-use or specific military standards. Efforts are being made to exploit civil-military synergies in the area of research and development. The EC has, in cooperation with EDA, recommended the development of so-called hybrid standards. Cooperation between civil and military organisations for standard development may experience issues due to security and classification.

On **European** level, the so-called Mandates (programming initiatives of the European Commission) are the most interesting, in particular mandates within the topic of security and/or disaster resilience which are issued to the European Standardisation Organisations (ESOs) CEN, CENELEC and ETSI. Five Mandates, have been selected for further analysis:

- M/419: Standardisation mandate addressed to CEN for the development of a series of standards on supply chain security
- M/487: Programming mandate addressed to CEN, CENELEC and ETSI to establish security standards
- M/509: Programming mandate to CEN, CENELEC and ETSI on protective textiles and personal protective clothing and equipment
- M/512: Standardisation mandate to CEN, CENELEC and ETSI for Reconfigurable Radio System
- M/530: Standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management

The analysis has shown that Mandates, if they should become successful and sustainable over the years of execution, require particular attention by all stakeholders involved to a number of critical issues and dependencies:

- *Framework conditions* — The timeframe and funding are different for each of the mandates and depend on the wishes of the requesting authority. Sufficient time and funding to execute the mandate work, but also to follow up on the top-down standardisation actions and recommendations, are essential for the success of such work.
- *Execution of the work* — Most mandates are addressed to the ESOs, to involve all European standardisation bodies in the work. The structure of the ESOs makes it challenging to involve all parties and to organise the execution of the work: often only one of the ESOs acts as the contact point, which makes it difficult to involve all of the ESOs. Also, as the ESOs themselves do not execute the work, often the secretariat of the related TC is asked to execute the mandate work. With all these layers (EC, ESOs, TC, WG, secretariat), the process to accept a mandate work and approval of the reports as a result of the work takes much time.
- *Stakeholder involvement* — Involving the ‘right’ stakeholders at the ‘right time’ for the ‘right level of involvement’ is challenging, in particular for topics in the area of security/disaster resilience, these horizontal subjects are even more difficult to cover with an even wider range of stakeholders (that are possibly only partially interested in the work). TC members represent experts from various European countries that are active in a specific area of standardisation. However, these experts represent only a part of the stakeholder community; sometimes specific groups of stakeholders are missing, such as end-users. Therefore, in the mandate work, a wider stakeholder involvement is included. However, despite or even because of the broad involvement of stakeholders, specific standardisation needs that resulted from the work were not always shared later on by the experts involved in standardisation.
- *Follow-up* — There is often a gap between the end of the mandate work and the uptake of the follow-up actions and recommendations. On the one hand, funding is not always available, resulting in a lack of time and resources for the follow-up. On the other hand, recommendations and actions concerning multiple areas of expertise and being relatively new to standardise, are found to be difficult to initiate.

Recommendations have been put forward for the ESOs and EC on how to address the above mentioned issues and dependencies based on the lessons learned from the PIs:

1. Monitoring of framework conditions
2. Setting a time frame
3. Simplifying processes
4. Ensuring consistent presence of stakeholders
5. Including a broad range of perspectives
6. Working in sub groups
7. Installing a horizontal platform
8. Ensuring funding
9. Preparing the uptake of the vision
10. Strengthen end-user involvement

Readers guide

Chapter 2 describes and analyses the civil and military PIs, distinguishing the national, European and international level. Furthermore, hybrid initiatives are also included in this chapter. Chapter 0 describes and provide an in-depth analysis of the European mandate M/487 “to establish security standards”. Chapter 4 presents the conclusions and recommendations of this work, where the main characteristics and lessons learned from the investigated European PIs in the field of security and disaster resilience are shown in Table 2.

Table of Contents

List of Tables	vii
List of Abbreviations.....	viii
1 Introduction	1
1.1 Objectives.....	1
1.2 Scope	2
1.3 Approach	2
2 Standardisation programming initiatives	4
2.1 Civil programming initiatives.....	4
2.1.1 National civil programming initiatives	4
2.1.2 European civil programming initiatives	6
2.1.3 International civil programming initiatives.....	20
2.2 Military standardisation	22
2.2.1 NATO standardisation.....	22
2.2.2 National military standardisation.....	23
2.2.3 Hybrid standards and M/512	24
3 Analysis and review of M/487	28
3.1 Preparation phase of mandate M/487	28
3.1.1 Description of the preparation phase.....	28
3.1.2 Review of the preparation phase.....	29
3.2 Implementation phases of mandate M/487	30
3.2.1 Description of the implementation phases	30
3.2.2 Review of the implementation phases	36
3.3 Follow-up of mandate M/487	38
3.3.1 Description of the follow-up	38
3.3.2 Review of the follow-up of M/487	40
4 Conclusions and recommendations	42
4.1 Conclusions for national programming initiatives	42
4.2 Conclusions for international programming initiatives	42
4.3 Conclusions for military programming initiatives	42
4.4 Conclusions and recommendations for European programming initiatives	42
Annex 1 Assessment sheet for identified PIs.....	48
Annex 2 BT N8625, including the draft resolution for CEN and CENELEC BT	50

List of Figures

Figure 1: Chronology of actions linked to mandate M/419	10
Figure 2: Chronology of actions linked to mandate M/509	15
Figure 3: Chronology of actions linked to mandate M/530	20
Figure 4: Procedures for development of standards in NATO (modified from Cihangir Aksit)23	
Figure 5: Involved organisations and representation	31
Figure 6: Timeline of actions linked to mandate M/487	31
Figure 7: Involved organisations for the execution of M/487 Phase 1	33
Figure 8: High level standardisation roadmap for border security	35
Figure 9: High level standardisation roadmap for crisis management	35
Figure 10: High level standardisation roadmap for CBRNE	36

List of Tables

Table 1: Input for ResiStand tasks coming from D1.2	1
Table 2: Investigated European programming initiatives in the field of security and disaster resilience.....	43

List of Abbreviations

CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CCMC	CEN CENELEC Management Centre
CEN/BT	CEN Technical Board
CSCG	Cyber Security Coordination Group (within CEN/CENELEC)
DG ENTR	Directorate-General Enterprise and Industry
DG HOME	Directorate-General Migration and Home Affairs
DG TREN	Directorate General of Transport and Energy
DIN	German Institute for Standardisation
DKE	German Commission for Electrical Engineering, Electronics and Information Technology
EC	European Commission
ETSI	European Telecommunications Standards Institute
EDA	European Defence Agency
ESOs	European Standardisation Organisations (CEN/CENELEC/ETSI)
IEC	International Electrotechnical Commission
ISO	International Organization for Standardisation
NEN	Netherlands Standardisation-institute
NSO	NATO Standardisation Office
PI	Programming Initiative
SDR	Software Defined Radio
SDO	Standard Developing Organisation
STANAG	Standardisation agreement (NATO)
TC	Technical Committee (within Standards Developing Organisations)
VDA	German Association of the Automotive Industry
VDE	Association for Electrical, Electronic and Information Technologies

1 Introduction

1.1 Objectives

The overall goal of the ResiStand Project is to find new ways to improve the crisis management and disaster resilience capabilities of the European Union and the individual Member States with means of standards. This objective will be achieved through:

- Proposing new standardisation activities that can advance and improve disaster resilience;
- Providing a better understanding of the potential of standardisation as a tool for improving disaster resilience;
- Presenting a new, sustainable process for better and faster capitalizing on the potential of standardisation.

To be able to achieve these goals, it is necessary to first understand the current way in which standards are initiated, developed and used. This deliverable (D1.2) focusses on the initiation of standards through Programming Initiatives (PIs), thus taking a “top-down approach”. The majority of standards, however, are initiated by stakeholders participating in standardisation committees, i.e. “bottom-up”. These stakeholders can be of all types: manufacturers, practitioners and end-users, engineers, quality control organisations, authorities, research and technology organisations, etc. Alternatively, the development of standards can be initiated by authorities through PIs. A lot of good work has been done with respect to programming of standardisation in the past. In this deliverable, applied processes and methodologies of PIs have been analysed and reviewed.

The intention of this deliverable is to learn from experiences with PIs and to provide this experience to the ResiStand Work Packages 1-6 to enable them to build up on what was positive and to avoid pitfalls.

Concretely, within the ResiStand project, this deliverable will provide input for the tasks as described in Table 1.

Next to the project internal audience, this deliverable is expected to be relevant for standardisation institutes and experts, e.g. those being members of the project’s SAG (Standards Advisory Group).

Table 1: Input for ResiStand tasks coming from D1.2

WP1 Establishing the project’s building blocks	
T1.3 Improved assessment framework for standardisation activities	Lessons learned from past standardisation PIs
WP2 Cross-sectorial screening and identification of resilience-relevant standards	
T2.2 Screening for and analysis of standards relevant for disaster resilience	Lessons learned from past PIs will be taken into account
WP3 Identification of standardisation needs and requirements	
T3.3 Consolidating, analysing, and updating needs of the E-UC (End-User Community)	Lessons learned from stakeholder workshops of past Programming Mandates will be taken into account
WP4 Identification of standardisation opportunities	
T4.2 Standardisation drivers and restraints of the industry	Lessons learned from previous initiatives with respect to stakeholder involvement processes.
T4.3 Standardisation drivers and restraints of the	Lessons learned from previous initiatives with respect to

research community	stakeholder involvement processes.
WP5 Preparation and roadmapping for standardisation activities	
T5.2 Identification of standardisation gaps	Lessons learned derived from the review of past and current PIs with respect to gap analyses.
T5.3 Assessment of proposed and planned standardisation activities and roadmapping for future standardisation activities	Lessons learned derived from the review of past and current PIs with respect to roadmapping activities.
WP6 Towards a sustainable process	
T6.1 Concluding the ResiStand Process to improve future standardisation work	Lessons learned derived from the review of past and current PIs with respect to the overall process of programming and the implementation of the recommendations stemming from the PIs.

1.2 Scope

Within the ResiStand project, a PI is considered to be a request from an authority to one or multiple organisations or persons, to investigate which standards should or could be developed in the future to bring solutions for current technical and non-technical challenges. PIs can be issued by all types of authorities, being international, European, national. This deliverable addresses in particular European PIs, focusing on subjects related to disaster resilience and crisis management, but international and national initiatives are discussed as well.

On the European level, the European Commission (EC) initiates standardisation activities through so-called “mandates”. These mandates can be divided in programming mandates and standardisation mandates. In programming mandates for standardisation, the European Standardisation Organisations (ESOs) are requested to investigate which standards could or should be developed in the future to solve a challenge or need specified by the EC. In standardisation mandates, the EC requests the European standardisation organisations to develop specific standards. The ESOs are the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI). The ESOs cooperate and coordinate as much as possible with the International Organization for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

This deliverable focusses mainly on programming mandates for standardisation. However, if relevant lessons can be learnt from standardisation mandates, those will be touched upon as well. The European PI M/487 ‘Programming Mandate addressed to CEN, CENELEC and ETSI to establish security standards’ is discussed in more detail than the other PIs, since this initiative is the most relevant one to disaster resilience and crisis management.

The analysis itself focuses on the processes and methodologies applied in the PIs. The particular aspects of feasibility and impact assessment of standardisation activities within the scope of PIs will be dealt within D1.3 “Assessment framework for standardisation activities”.

In chapter 2 of this document, civil and military PIs are described and analysed, distinguishing the national, European and international level. Furthermore, hybrid initiatives are described.

The European programming mandate M/487 to establish security standards is described and analysed in depth in chapter 0. Chapter 4 finally contains the conclusions and recommendations.

1.3 Approach

The majority of the information has been obtained through desk research. PIs have been analysed, using the assessment sheet developed by the partners. An assessment sheet was developed that allowed to structure the information obtained and to divide it into information regarding the preparation, the implementation and the sustainability of the PI. The main characteristics and lessons learned from the investigated European PIs in the

field of security and disaster resilience are shown in Table 2, which is part of chapter 4 Conclusions and Recommendations.

To be able to review the preparation of the PIs, the motivation for the PI and the design of the PI were analysed. For the review of the implementation of the PIs, the organisation of work and the results of work were analysed. Finally, for the review of the sustainability of the PI, the implementation of results, the continuation of results after the exploration of the PI and the follow-up were analysed. For this assessment sheet, see 0.

To get a complete overview of the process followed for M/487, informal exchanges of views with persons involved have been conducted. These persons represent Directorate-General Migration and Home Affairs (DG HOME) Unit B.4 Innovation and industry for security (previously responsible for issuing the mandate, as a unit of Directorate-General Enterprise and Industry (DG ENTR) at that time), CEN CENELEC Management Centre (CCMC) and the Netherlands Standardisation-institute (NEN) (executing the mandate).

2 Standardisation programming initiatives

2.1 *Civil programming initiatives*

In this section a selection of civil PIs which are aiming to investigate and/or develop standardisation deliverables to support efficient and reliable products, services, processes etc. is analysed. The main focus is laid on PIs in the security area, especially when it comes to the core topic of ResiStand – disaster resilience and crisis management – but is not limited to that. Initiatives on national, European and international level are considered.

2.1.1 *National civil programming initiatives*

On national level the existence of civil PIs in the field of security and disaster resilience has been investigated. Therefore a survey among members of CEN Technical Committee (CEN/TC) 391 'Societal Citizen Security' was initiated. Based on the obtained responses and the conducted desk research there have not been identified any national PIs requesting the investigation of the need for or the development of standards within the context of security and disaster resilience in Germany, U.K., Italy, Austria, Czech Republic, Netherlands, Sweden, Norway and Finland.

However, apart from national PIs in the field of security and disaster resilience, one initiative about electric mobility in Germany has been found interesting in particular. Even though this does not relate to disaster resilience, it showed some useful aspects which could be transferred to other sectors.

Similar to the security sector, electric mobility is a very cross-sectional topic. Stakeholders from different industries as e.g. automotive, battery-technology, information and communication technology (ICT) and energy supply are involved in the current transition phase from the conventional petrol or diesel engine concept towards a more sustainable electric car concept. Since a lot of stakeholders are affected by the topic and vice versa, this transition is a very complex process. Additionally many innovative actions, which need to be synchronised, are in progress in Germany, Europe and around the world. Similar to other sectors, standardisation can play a crucial role when it comes to a smooth and efficient introduction of new technologies as those linked to electric mobility.

When it comes to standardisation in the cross-sectional area of electric mobility one can not only find a huge number of stakeholders involved but several standardisation committees working on different aspects. In Germany, the German Institute for Standardisation (DIN) takes responsibility for the development of standards. This comprises the coordination on national and international level through the electromobility office, established at DIN in 2009, as well as the technical standardisation work conducted by the German Commission for Electrical Engineering, Electronics and Information Technology in DIN and VDE (DKE), and by the automotive standards committee within the German Association of the Automotive Industry (VDA).

In 2009 the German Federal Government published the 'Federal Government's National Development Plan for Electric Mobility' which led to the foundation of the German "National Platform for Electric Mobility" (NPE).¹ The NPE functions as an "advisory body of the Federal Government [and] brings together 150 representatives from industry, science, politics, trade unions and trade associations for strategic dialogue. Collectively, they investigate the economic, social and environmental potential of electric mobility and recommend actions for

¹ <http://nationale-plattform-elektromobilitaet.de/en/>, July 2016

politicians and business."² Original seven working groups have been established. One of which is Working Group 4 – 'Regulation, Standardisation and Certification'. DIN, DKE and VDA are observers in the working group but DIN supervises its steering committee which is responsible for preparing topics and giving recommendations of action as a neutral party to the group. One essential output of Working Group 4 is a standardisation roadmap for electromobility which is part of a general electromobility roadmap developed by the NPE. In 2014 the third edition of the standardisation roadmap for electromobility has been published and currently a complementing roadmap 4.0 is under way. The roadmap identifies the current standards inventory and the need for future extension respectively adaption of the existing portfolio. It is even giving specific recommendations e.g. on how to revise certain standards. Those recommendations are actively followed within the different technical standardisation committees of DIN, DKE and VDA. New standards and updated existing standards are some of the major outputs of the collaborative work done in the framework of the NPE.

Additionally, the Federal Ministry of Economics and Energy (BMWi) funded several projects, e.g. a project called 'E-moNorm' to promote electric mobility through standardisation, coordination and increasing the public awareness. DIN coordinated these projects; while VDE (DKE) and VDA (with the automotive standards committee) are additional project partners. The strategic objectives of the project are:

- implementation of the German standardisation roadmap for electromobility,
- integration of research and development project results into the standardisation process,
- early identification and integration of new standardisation topics,
- development of strategic alliances, and
- support of German small and medium sized enterprises (SMEs).

To summarise, broad networking including the involvement of all stakeholders and early identification and implementation of potential standardisation topics are key elements. After all, electric mobility is a global concept meaning there can be no limit to the German perspective only. Internationally, DIN, DKE and VDA are cooperating e. g. with US-American³, Japanese and Chinese⁴ entities which are mostly but not only standardisation bodies. Partly, one strategic approach followed by the German standardisation organisations and the related stakeholders is to develop standards in specific areas for electric mobility on national level first and bring forward the document as a proposal to the European or international level as a next step. Here the advantage lies in the quick consensus-finding and standard-developing process for the basis document on national level.

In essence one can say that, in the framework of the NPE and funded projects as E-moNorm, DIN DKE and VDA are functioning as moderators, organisers and contact points for any topics related to standardisation in the field of electric mobility. The overall goal of all these activities and initiatives is to increase the acceptance for electric mobility on the market to support the climate targets of the national government and support the national automotive industry to be a global market leader in the future.

Lessons identified and learned

A few aspects of the German electric mobility standardisation framework are worth highlighting. First of all there obviously is a strong support by the national government which did initiate a platform to push forward the electric mobility technologies and its market penetration. This platform brings together all relevant stakeholders. In terms of pre-normative activities projects as 'E-moNorm' have been funded by the national government continuously since 2010. The main tasks of the project and the involved organisations (DIN, DKE, VDA) are to monitor and integrate relevant research activities; monitor existing standards and ongoing standardisation activities on national, European and international level; and be a contact point for stakeholders when it comes to any aspects concerning standardisation in the field of electric mobility. Furthermore, the SDOs support the

² <http://nationale-plattform-elektromobilitaet.de/en/the-npe/organisation/>, July 2016

³ E.g. Society of Automotive Engineers (SAE)

⁴ E.g. Standardization Administration of the People's Republic of China (SAC)

continuous development and revision of a standardisation roadmap for electromobility. An international collaboration considering initiatives in e.g. China, India or Japan is particularly formed. Short-term needed and as important marked standardisation topics are partly developed on national level first and being proposed as a European or international standardisation deliverable afterwards. The system implemented here is working well and continuously adapting to the changing working environment.

2.1.2 European civil programming initiatives

If European policies and legislation require standardisation, the EC in a top-down approach is able to request the ESOs to develop and adopt such European standards, by issuing requests in form of mandates⁵ to the ESOs. If standardisation needs are not yet specifically identified, a mandate can be issued, in order to initiate the development of a future standardisation work programme by the ESOs. Specific standardisation requests based on the work programme can be issued in a second step. If the EC wants to request standardisation activities in this way, it has to publish the planned actions in its annual Union work programme for European standardisation (AUWP) before.

On European level, the described work of the EC is most influential. In particular mandates within the topic of security and/or disaster resilience which are issued to the European Standardisation Organisations (ESO) CEN, CENELEC and ETSI are of interest.

In the following clauses, the formerly issued mandates M/419, M/509 and M/530 are analysed. M/487 is assessed in detail in chapter 0.

Additional initiatives as

- 'European Standards for the space industry' (M/237; M/415; M/496),
- 'ICT Standardisation Priorities for the Digital Single Market',
- Mandate M/355 'Programming mandate addressed to the European standardisation organisations for the elaboration of European standards to identify and reduce crime risk in products and services',
- 'Implementing the European Agenda on Security: EU action plan against illicit trafficking in and use of firearms and explosives' and the
- 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'

have been identified but not investigated within this report.

2.1.2.1 Mandate M/419 – Standardisation mandate addressed to CEN for the development of a series of standards on supply chain security

Preparation phase

In the years after the terrorist attacks on 9/11, 2001 in the USA, the EC Directorate General of Transport and Energy (DG TREN) started a proposal for a regulation enhancing the cargo surface transport security. A set of new customs, aviation and maritime supply chain security regulations, programs and standards, in the USA, Europe and across the globe was established. In the area of road and rail cargo, however, there was still a lack of regulations until EC DG TREN started the "Secure Operator" initiative in 2004.⁶

An article published by the Cross-border Research Association mentions: "By 2006, the main goal of the EC proposal for a regulation on enhancing supply chain security (SCS) in the EU was shaped as to achieve greater protection of the European freight transport system against possible terrorist attacks. The specific objectives of the draft regulation were defined as: (i) to increase the level of security along the supply chain without impeding the free flow of trade; (ii) to establish a common framework for a systematic European approach without

⁵ Various terms are used for these types of request, such as 'Standardization Mandate', 'Programming Mandate' and 'Standardization request'. This document will refer to 'Mandate' in all these cases.

⁶ <http://www.cross-border.org/2016/05/21/eu-logistics-security-an-interesting-decade/>, July 2016

jeopardizing the common transport market and existing security measures; and (iii) to avoid unnecessary administrative procedures and burdens at European and national levels. In addition, the draft regulation related to the need to prevent a patchwork of various supply chain security standards and solutions across EU."⁶

Complementing the EC established the European mandate M/419 'Standardisation mandate addressed to CEN for the development of a series of standards on supply chain security' in 2007. This was motivated by the perception that there is a gap in the area of security standards and legislations for EU internal market transport which causes vulnerabilities in the supply chain security. Member States tend to prefer the application of their own national security rules in order to react and adapt to individually experienced threats. This however contradicts the idea of a European single market in which companies are able to easily offer their solutions European-wide. European harmonized standards were identified as key in order to prevent the development and application of multiple supply chain security standards across Europe and support consistent security standards which fit all EU internal market requirements.

According to the mandate itself, the instrument of standardisation is identified crucial for its characteristics regarding transparency, impartiality, objectivity, openness to different stakeholders, operators, particularly SMEs. European standards are able to establish a minimum performance level for transport security in the EU internal market. This will support the Authorised Economic Operator⁷ (AEO) concept introduced by the World Customs Organisation (WCO) which aims to enhance international supply chain security.⁸

In the mandate it was pointed out that the EU security legislation has implemented several elements, e.g. on aviation security – (EC (2002)2320), maritime and port facilities – (EC (2004)725), ports – (EC (2005)65) and international trade – (Customs - EC (2005), 648, EC (2006)1875). However, for the supply chain in the EU internal market no security legislation was developed. There was a large amount of non-consistent standards including business standards which is hindering an effective trade with the EU in the international context and is a handicap especially in the EU-US trade. According to the EC Freight Transport Logistics Action Plan – (COM (2007)607), European standards can contribute to the fine-tuning and interconnectivity between existing EU initiatives and legislation on transport security.⁸

Summarised, the expected impact was to enhance security in the supply chain; define most effective and cost-effective measures; develop a method for supply chain vulnerability assessment; allow tailor-made and cost beneficial security measures and streamline different terminologies on supply chain security statuses.⁸

Mandate M/419 was issued to the European Committee for Standardisation (CEN) with the task to investigate the necessity and feasibility of the development of European standards, the foreseen impact of potential standardisation deliverables and the actual development of standards in the field of supply chain security, when found appropriate.⁸

The foreseen result of executing the mandate was a set of standards that could be used as a toolkit by organisations of any size to evaluate the adaptability of their management and security measures to official security levels.

An expert group on supply chain security was already in place under CEN working group "Protection and Security of the Citizen" (CEN/BT/WG161)⁹. In regard to M/419 as a first action the group was meant to compile a report framing actions that would support the work of the relevant technical body. The EU Logistics Action Plan was strongly considered in the process. Additionally the Cross-border Research Association, which is an independent research institute focusing on advanced supply chain security, crime prevention, risk management, cross-border trade and logistics, trade facilitation, coordinated border management, and public-private co-operation

⁷ For more information see:

http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/aeo_en.htm#what_is , July 2016

⁸ M/419 Standardisation mandate addressed to CEN for the development of a series of standards on supply chain security, Brussels, 23 November 2007

⁹ <http://www.cross-border.org/2016/05/21/eu-logistics-security-an-interesting-decade/> , July 2016

research, training and consulting, was consulted by the expert group.¹⁰ The report was published at the end of 2006. The CEN Technical Board (CEN BT) approved the findings and supported the development of standards on operational supply chain security.

The mandate requested a detailed work programme and a timetable to be handed over to the EC by CEN within three months after acceptance of the mandate. It further asks for the adoption of the standard(s) within three years after the acceptance of the mandate.

It was recommended to involve representatives of operators in the supply chain and public authorities that have shown interest in the development of the standard(s) as appropriate. Some organisations as CLECAT¹¹, ESC¹², ESPO¹³, ESBA¹⁴, EPSO¹⁵, TAPA¹⁶, Eurocommerce, consumers' interests (ANEC¹⁷), environmental protection (ECOS¹⁸), workers (ETUI-REHS¹⁹) and small and medium-size enterprises (NORMAPME²⁰) have been mentioned specifically.

Implementation phase

The CEN expert group for supply chain security was requested to give guidance on the actual standardisation related work to be done following mandate M/419. In December 2007 this expert group was renamed into CEN/TC 379 'Supply Chain Security'. The secretariat of the TC was held by NEN. During that time there was an enquiry phase regarding the formal acceptance of mandate M/419. A NORMAPME newsletter from March 2008 describes: "The mandate is much less prescriptive than usual and will leave TC 379 ample room for its own concepts. Members of the TC 379 were requested to send their comments with regard to the mandate to the secretariat before 14 March 2008. NORMAPME already submitted comments on the draft mandate in December 2007. After having carefully read the final mandate, a further comment on the representativeness of small and medium sized enterprises (SMEs) in the transport field was added to the former NORMAPME comments. Acceptance of the mandate by CEN will take place after positive vote by the members of the Technical Board at CEN."²¹ The mandate was voted positive and thereby accepted by CEN BT.

As a next step the Cross-border Research Association was requested to conduct a feasibility study on supply chain operators needs for a possible European standard in supply chain security. The study was funded by DG TREN and contracted by CEN. It was published in 2010 and made three main recommendations regarding the future of supply chain security standardisation in Europe²²:

1. Development of a CEN standard for crime incident reporting in Europe. This standard can be exploited to harmonize the interaction between business and relevant authorities throughout Europe, in particular for reporting of crime incidents; and to streamline and speed up the process of collecting and sharing data on crime incidents, for the benefit of both supply chain operators and authorities.

¹⁰ <http://www.cross-border.org/>, July 2016

¹¹ European Association for forwarding, transport, logistics and customs services

¹² European Shippers' Council

¹³ European Sea Ports Organisation

¹⁴ European Small Business Alliance

¹⁵ European Personnel Selection Office

¹⁶ Transported Asset Protection Association Europe

¹⁷ European consumer voice in standardisation

¹⁸ European Environmental Citizens Organisation for Standardisation

¹⁹ European Trade Union Institute for Research, Education and Health and Safety

²⁰ European Office of Crafts, Trades and Small and Medium-sized Enterprises for Standardisation (NORMAPME) was created in 1996 by the European Association of Craft, Small and Medium-sized Enterprises (UEAPME)

²¹ http://www.fp7-aspire.eu/fileadmin/aspire/docs/34_NI_Mars_08_en.pdf, July 2016

²² https://www.unece.org/fileadmin/DAM/trans/events/docs/inlandsecurity_forum11_relatingmaterial_01e.pdf, July 2016

2. Development of a good practice guidebook on SCS, sharing experiences between supply chain operators as to which security measures work (in which contexts), about the costs and benefits, and other relevant parameters, to be exploited in SCS design, implementation, monitoring and training.
3. Carrying out a set of detailed cost benefit case studies. These focus on a holistic SCS label, targeted primarily for European small and medium sized enterprises (SMEs) in the logistics sector, especially for companies which are not eligible for customs SCS programs (like EU AEO). Based on the outcomes of 20-30 case studies, this additional study suggests the final decision as to whether a SCS label type of standard will or will not work.

Additionally the study suggested a holistic supply chain security framework to be considered in future standardisation projects in the field. It proposed main focus points, priorities and stakeholders for future activities based on findings in the literature, in expert interviews, in in-depth SCS initiative analysis, and/or in a conducted operator survey.²¹

On the political stage it became clear that EU Member States did not support common supply chain security regulations in the context of terrorism to surface transport in 2010. The countries and different stakeholders were focusing on their particular interests and would not support an approach considering a holistic supply chain picture. Thus the regulation was blocked in the European legislative process and finally withdrawn by the EC in 2010.²³

For instance, UEAPME²⁴ which is connected to NORMAPME²⁰ wrote a position paper from October 2012: "UEAPME TF strongly opposes the Commission's idea of introducing a European standard for "end-to-end security", and all reanimation of this topic. The European Committee for Standardisation, CEN TC 379 on supply chain security concluded, after years of study work, that a standard was not needed and a voluntary good practice guidebook was found sufficient."²⁵

However, UEAPME supported recommendations 1) and 2) of the Cross-border Research Association's study.²⁵

In 2012 the CEN Technical Report CEN/TR 16412:2012 'Supply Chain Security – Good Practice Guide for Small and Medium Sized Operators' was published by CEN/TC 379, serving recommendation 2) of the study. About the Technical Report UEAPME writes: "SME's are best served by a voluntary good practice guidebook made and used by operators. The guidebook will serve as a low cost and user-friendly tool."²⁵

Later in 2013 another European Standard EN 16352:2013-06 'Logistics – Specifications for reporting crime incidents' was published considering recommendation 1) of the study. "In situations where a driver is robbed in Europe, he has to report the incident to the local police. This is often difficult due to language problems. The standard provides a form with questions to be filled in by the driver, this eases the process of reporting the robbery."²⁶ UEAPME writes: "The use of the report form will make it possible to set up a central databank with registration of all transport related crime incidents. This databank will be an important tool in prevention of incidents and will make transport criminality more visible."²⁵

In 2014, after publishing the European Standard, CEN/TC 379 was disbanded and did not further work on any standard. On recommendation 3) there has not been found evidence about any work completed or in progress.

An overview on the chronological list of main actions regarding Mandate M/419 is provided in Figure 1.

Interestingly on the global level, ISO 28000 series on supply chain security was published between 2007 and 2015 by ISO/TC 292. It includes e.g. recommendations on design, evaluation and requirements for secure supply

²³ <http://www.cross-border.org/2016/05/21/eu-logistics-security-an-interesting-decade/>, July 2016

²⁴ The European Association of Craft, Small and Medium-sized Enterprises

²⁵ <http://www.ueapme.com/IMG/pdf/121030UEAPMEpositionTransportSecurity.pdf>, July 2016

²⁶ http://crispproject.eu/wp-content/uploads/2014/10/CRISP_Deliverable_2-1_Sec_Standards_Certification_Europe-Compressed.pdf, July 2016

chains. They have not been adopted in the European set of standards. Even though, several European certification bodies²⁷ use the international ISO 28000-series for certification.²⁶

Follow-up

Since the publication of EN 16352:2013-06 and CEN/TR 16412:2012 there have not been any further activities connected to CEN/TC 379 as it was disbanded. The mandate M/419 has been finished to that point and no further work is envisaged on European level. However, other supply chain security related activities are taking place such as further work on the ISO 28000 series and the development of DIN CWA 17056.

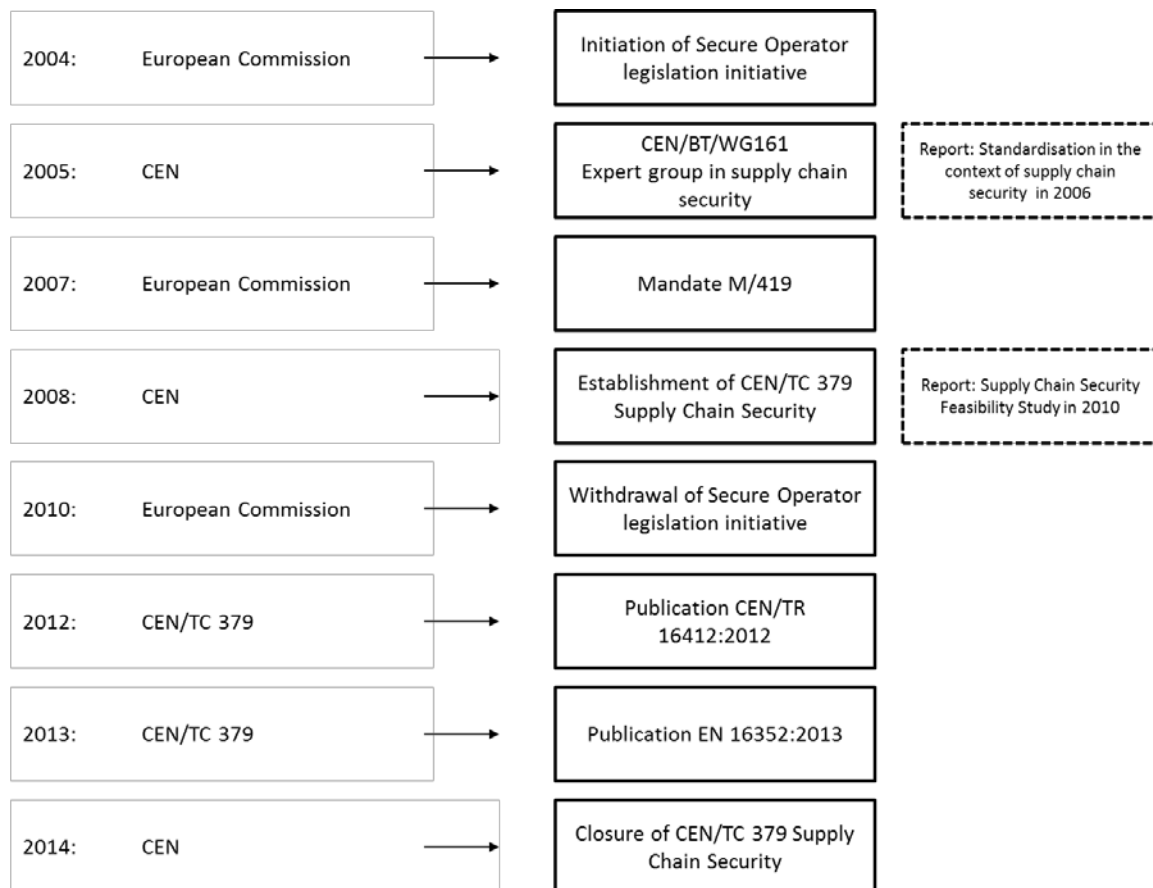


Figure 1: Chronology of actions linked to mandate M/419

Lessons identified and learned

Clearly mandate M/419 was responding to specific threats which appeared to be present at the time given. When the 'Secure Operator Legislation Initiative' was initiated it built the basis for following activities such as the mandate. At CEN a task force was introduced in order to identify actions for supporting future standardisation activities in the field of supply chain security. From the available information it is not clear which stakeholders were part of the task force and who was involved in the preparation of the mandate. Specific recommendations about stakeholders to be involved in the execution of the mandate were given. It might be assumed that those stakeholders were involved in the preparation phase as well. It is also not clear to which degree the SDOs and ESOs have been consulted when preparing M/419. After the acceptance of mandate M/419 the following study

²⁷ Among others: Lloyds, Veritas, SGS, TUV, DNV

mainly conducted by a standardisation external research group served as a detailed basis for the specifically convened CEN/TC 379. Here, funding by DG TREN was available. Detailed interviews with relevant stakeholders have been conducted. The study addressed the points mentioned in the mandate and as a result three main recommendations regarding the development of standardisation deliverables have been given to CEN/TC 379. Subsequently two of the three recommendations have been put into practice.

Considering all, the work has been executed as stated in the mandate, even though the timeframe given was not met. The specific need for standards in the field has been investigated and the actions derived from the conducted study have been put in practice as far as possible. The SDOs and ESOs have been utilised to include relevant stakeholders for investigating the need of standards. However, given the efforts that have been put into the whole initiative the overall results are rather limited. The expected impact of M/419 in terms of e.g. terminology, vulnerability assessment and cost efficiency has not been fully met. In the execution of the mandate the former mentioned political-driven top-down approach seems to have been partly taken down by the stakeholder communities which did not see the need for a holistic standards framework in the field of supply chain security. One could imagine that an intensive early stakeholder involvement could facilitate a good effort/benefit ratio. It can be expected that the withdrawal of the 'Secure Operator Legislation Initiative' did not show a positive impact on the standardisation efforts. Within the work done when executing M/419, ISO activities seem not having been strongly considered. In the same time some influential standards have been developed on international level, not being adopted into the European standards inventory. In 2014 CEN/TC 379 has been closed down and is not active anymore. In terms of sustainability of the initiative surrounding mandate M/419 no further activities are to be expected in the near future.

2.1.2.2 Mandate M/509 – Programming mandate to CEN, CENELEC and ETSI on protective textiles and personal protective clothing and equipment

Preparation phase

In 2007 the Lead Market Initiative²⁸ (LMI) was launched in order to identify potential future fast growing markets and facilitate access to them for Europe. The goal was to enter those as early as possible to become a pioneer and gain competitive advantages for Europe in the future. Following a call for identification of promising markets, "the European Technology Platform for the Future of Textiles and Clothing (Textile ETP) launched an internal survey to identify suitable textile-related lead market candidates. This led to the eventual endorsement by the Textile ETP's industry-led Governing Council of "Intelligent Personal Protective Clothing and Equipment" as a proposal to the EC."²⁹

In December 2007 the EC published the Communication named 'A lead market initiative for Europe'. Six markets had been identified for Europe to be a leading market innovator in the future. One of the six identified markets has been the field of protective textiles.

A task force was built and issued with the task to compile a strategy which was later published in a report called 'Accelerating the development of the protective textiles market in Europe'. A close link between personal protective equipment (PPE) and protective clothing has been identified considering the 1989 European Directive 89/686/EEC. However, the concept of protective textiles has a broader scope than the directive and legislation in general defines. Products in the area of protective textiles "are used for professional workers, emergency services, defence personnel or healthcare professionals exposed to hazardous environments, extreme climatic conditions or chemical and bacterial contamination".³⁰

²⁸ COM (2007) 860 final, Brussels 21.12.2007

²⁹ <http://www.textile-platform.eu/lead-market-protective-textile/> , July 2016

³⁰ M/509 Programming mandate to CEN, CENELEC and ETSI on protective textiles and personal protective clothing and equipment, Brussels, 2012

An action plan for protective textiles to coordinate action areas of legislation, standardisation, public procurement and complementary activities was agreed on among various stakeholders in 2008 and implemented since.³⁰

The EC started funding several research projects under the 7th Framework Programme (FP7) as well as ENPROTEX, a public procurement network. Standardisation was identified as one of the key instruments in order to promote innovative advances in the field.³⁰

In 2012 mandate M/509 'Programming mandate to CEN, CENELEC and ETSI on protective textiles and personal protective clothing and equipment' was developed and published by the EC to support the development of standards in the field of protective textiles and personal protective clothing and equipment.³⁰

Its objective was the development of standardisation deliverables and revision of existing European standards in the area of protective textiles and personal protective clothing and equipment.³⁰

In this regard the EC asked specifically to investigate the potential of standards for three main topics:

- "Compatibility of different elements is crucial to ensure effectiveness of advanced, smart integrated protection systems. This includes compatibility of different system components and especially when ICT, other electronics and other advanced technologies are integrated in advanced PPE.
- Ergonomics and comfort are essential requirements for PPE to deliver the targeted level of safety and well-being in intended operating conditions. However, the assessment of such requirements relies on costly and frequently subjective testing methodologies; therefore, there is a need to explore and develop testing methods which are simple, objective and cost-effective. Virtual testing and simulation offer a potential yet under exploited in this area.
- Environmental sustainability and the total cost of ownership (lifecycle cost approach) are increasingly drivers of innovation in private and public PPE markets. In this context, it is necessary to develop methodologies to assess the total cost of ownership (or lifecycle cost) as well as the environmental impact throughout the lifecycle of products, including recycling and end-of-life disposal. The total cost of ownership should take into account not only the costs and impacts linked to the product supply chain but also those related to services (care and maintenance) that are critical for preserving the functionalities and ensuring optimal performance."³⁰

At CEN a Personal Protective Equipment (PPE) Sector Forum was established in connection with European Directive 89/686/EEC to coordinate European standardisation in the field of PPE long before the lead market initiative or mandate M/509 had been developed. These initiatives were expected to be considered when executing the tasks described in M/509 as follows:

- "Further explore and identify key recent technological developments for the deployment of smart integrated protection systems which integrate ICT, other electronics and other technologies in protective textiles, clothing and equipment.
- Identify cross-cutting barriers and drivers for the integration of technological developments resulting from R&D projects into new standards (or other standardisation deliverables). Among others, such barriers may include differing intellectual property right (IPR) management or protection of personal data.
- Explore existing standards in the field of ergonomics and comfort in order to identify whether recent technological developments and smart integrated protection systems would require further standardisation in this field.
- Explore existing methodologies to assess the overall lifecycle cost of protective textiles, clothing and equipment as well as the overall environmental impact in order to identify further standardisation needs.
- Establish a programme of standardisation deliverables, including Technical Reports and Technical Specifications that could eventually lead to European Standards for the three areas:
 - Advanced integrated smart protection systems
 - User-driven ergonomics and comfort

- o Assessment of lifecycle cost and environmental impact³⁰

Work items supporting essential requirements of Directive 89/686/EEC as harmonized standards should have been identified as well as any needs to develop new test methods in the area.³⁰

The mandate requested a detailed work program and a timetable to be handed over to the EC by CEN within 12 months after acceptance of the mandate.³⁰ End dates for the mandate in order to e. g. submit any deliverables or similar have not been announced.

When conducting the work described in M/509, the ESOs were expected to particularly coordinate between themselves including all relevant TCs. Moreover findings of EU funded projects e.g. under FP7, international activities as e.g. at ISO-level and relevant European Technology Platforms should have been considered strongly.

Advice on including the European Agency for Safety and Health at Work (OSHA) and representatives of consumers' interests (ANEC), environmental protection (ECOS), workers (ETUI), SMEs (NORMAPME), the European Federation of Textile and Clothing industry (Euratex), the European Safety Federation (ESF), and the European Textile Service Association (ETSA) was given.

Implementation phase

Mandate M/509 was approved on the 8th of November 2012 by CEN and CENELEC, and a new BT working group, CEN-CENELEC BT WG 8 'Protective Textiles', was established with the objective to develop a work programme in response to the mandate. ETSI did not accept the mandate, considering it not of relevance to them.³¹

In January 2013 the kick-off meeting of the CEN-CENELEC BT WG 8 was organised. Convenors and secretaries of relevant TCs as well as representatives of different stakeholder groups and R&D projects were invited to the meeting.

The relevant TCs were:

- CEN/TC 79 – Respiratory protective devices,
- CEN/TC 85 – Eye protective equipment,
- CEN/TC 158 – Head protection,
- CEN/TC 159 – Hearing protectors,
- CEN/TC 160 – Protection against falls from height including working belts,
- CEN/TC 161 – Foot and leg protectors,
- CEN/TC 162 – Protective clothing including hand and arm protection and lifejackets,
- CEN/TC 136 – Sports, playground and other recreational facilities and equipment,
- CLC/TC 78 – Equipment and tools for live working.

Those committees are members of the PPE Sector Forum as well.

ISO/TC 94 'Personal safety – Protective clothing and equipment' has been identified as a TC on international level whose work should be considered in that regard as well.

Additionally the National Standards Bodies (NSB's) received invitations to nominate experts. 35 participants were present at the kick-off meeting and it was decided to build four task groups to divide the work expected according to the mandate and facilitate an efficient way forward since time for execution was limited to one year.³¹

Those task groups were:

- TG 1: Compatibility of different elements – Technology,
- TG 2: Compatibility of different elements – Integration of the complete system,
- TG 3: Comfort and ergonomics,

³¹ Programming Mandate M/509 – Protective textiles and personal protective clothing and equipment, Final Report

- TG 4: Environmental sustainability and total cost of ownership.

After the first round of meetings of the different TG's existing relevant documents (European or other) were identified and proposals for future standardisation work were prepared. Two plenary meetings of CEN-CENELEC BT WG 8 took place in 2013 with a participation of about 30 experts from around Europe and from different stakeholders.³¹

The final report on Programming Mandate M/509 – 'Protective textiles and personal protective clothing and equipment' by CEN-CENELEC BT WG 8 was published in January 2014.

A number of proposals for future standardisation activities had been identified and prioritised on basis of three main criteria: priority in the sense of how urgent the standard is needed; anticipated cost to develop the standard; timeframe in the sense of time needed from start of development to publication of the standard. The proposals were forwarded to the respective TCs.³¹

"In addition [...] other proposals are also included looking towards improving the organisation of the standardisation work itself [e.g. participation of end users and R&D community in the standardisation process], improving uniformity of testing and quality of test methods, as well as on the conformity assessment protocols necessary for PPE having to comply with different sets of European legislation."³¹ It is mentioned in the report that the "programming mandate has created a renewed interest and momentum in the PPE sector as a whole."³¹

The report stressed that the current structure of TCs concerned with PPE is based on a set of product groups. The PPE Sector Forum was established to improve coordination between these TCs but is limited to coordination tasks only since it does not have the competence to prepare any standardisation deliverables.³² The final report recommended setting up "a complementary horizontal TC to deal with issues looking from a user perspective. Simultaneously the TC could be tasked to establish 'user groups' that have the task to clearly define the user needs as an input for the work of the product TCs."³¹

Considering that, NEN put forward a proposal for establishing a new horizontal CEN/CENELEC/TC in the field of Personal Protective equipment in July 2015. The tasks of the TC to be established are suggested as: developing Technical Reports describing user needs; cooperating with existing PPE products TCs; providing guidance to users on various topics; connecting to the international standardisation work.³² Many experts which have been involved in the when compiling the final report on M/509 show interest and engage in the implementation phase of the recommendations.

The proposal was circulated for voting till October 2015.³³ The result of the voting was negative due to a fundamental disagreement by the Swedish standardisation organisation and less than 5 countries that wanted to participate actively in the work of the new TC. CCMC concluded that the PPE Sector Forum had to be asked to formulate a strategy for the PPE sector. In August 2016 the process of defining this strategy is finished. It will be sent to the CEN-CENELEC BT WG 8 by autumn 2016. NEN is then going to rewrite the TC proposal and launch it again.

In the CEN/CENELEC work programme 2016 the PPE sector is presented with a section stating that a number of standardisation activities proposed by CEN-CENELEC BT WG 8 will be started during the year. Additionally "CEN has set up a new Working Group under CEN/TC 122 'Ergonomics', which will develop deliverables in relation to 'ergonomics design and evaluation of integrated PPE systems'."³⁴

³² NEN proposal for a CEN/CLC/TC on 'Personal Protective Ensembles and Systems', 2015, See <https://www.standard.no/Global/PDF/Standardisering%20-%20nye%20prosjekter/personal%20protective%20ensembles%20and%20systems.pdf>

³³ In the preparation phase of the proposal NEN and AFNOR both were drafting separate proposals for a new TC. These have been merged and submitted by NEN at the end.

³⁴ CEN and CENELEC Work Programme 2016, See http://www.cen.eu/news/brochures/brochures/CEN-CENELEC-WP2016_EN.pdf

In March 2016 Regulation (EU) 2016/425³⁵ were adopted superseding Council Directive 89/686/EEC on which basis mandate M/509 and many of since then established harmonized standards have been developed. The new regulation has been adopted in order to "[...] reflect current technologies and processes for developing and bringing PPE to the market [...]".³⁶ There is a two-years transition phase for EU Member States and concerned stakeholders to prepare the introduction of the new Regulation.³⁶ The CEN/CENELEC PPE Sector Forum was and is cooperating with the EC regarding the transition which affects a number of harmonised standards. "The overall objectives of this initiative are to (1) better protect the health and safety of PPE users, (2) create a level playing field for PPE economic operators and (3) simplify the European regulatory environment in that field."³⁷ Since the introduction of Council Directive 89/686/EEC in 1989 numerous regulations have become effective. With the revision of the PPE directive these are considered in an appropriate way.

However, a Commission Staff Working Document on the impact assessment of the new regulation reveals that all the identified deficiencies of the PPE Directive are of minor significance.³⁷ Thus, the impact on mandate M/509 and standardisation work can be expected to be rather small.

Figure 2 provides an overview on the chronology of main actions regarding M/509.

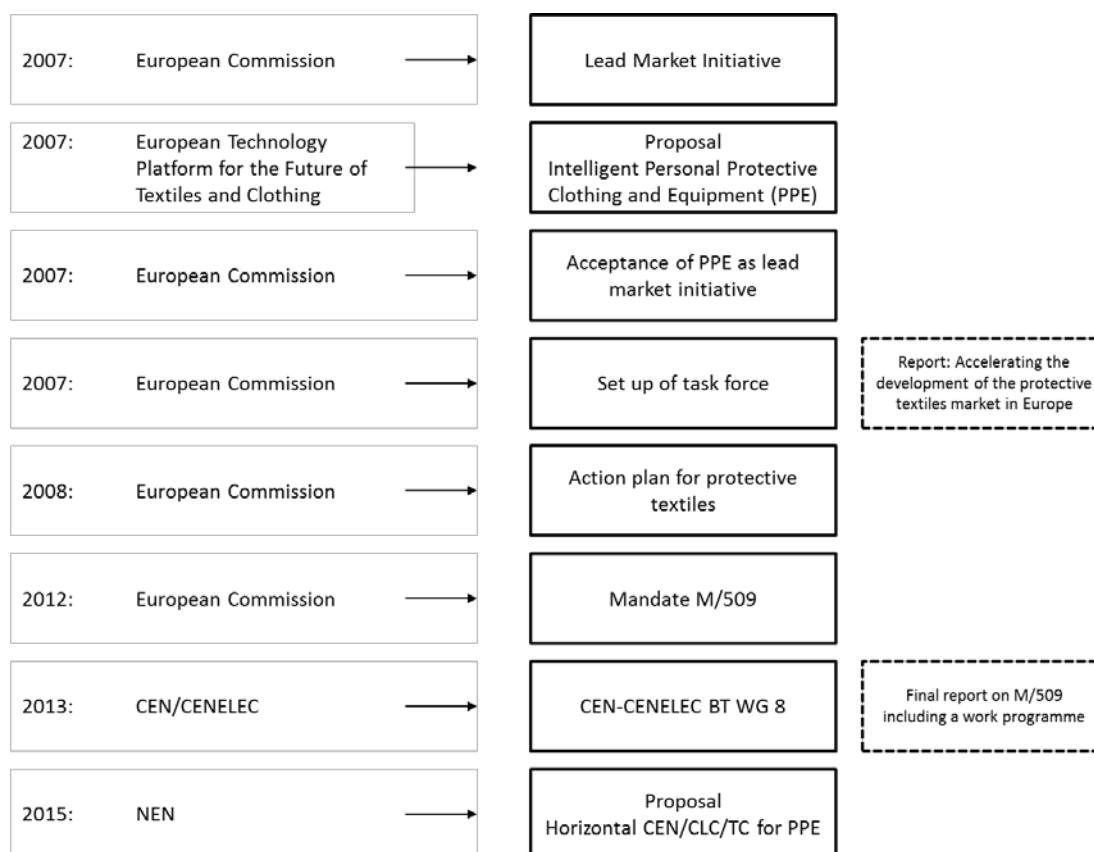


Figure 2: Chronology of actions linked to mandate M/509

³⁵ <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0425&from=EN> , July 2016

³⁶ <http://www.bsigroup.com/Documents/BSI-PPE-Whitepaper-UK-EN.pdf> , July 2016

³⁷ http://www.parliament.bg/pub/ECD/151382SWD_2014_118_EN_DOCUMENTDETRAVAIL_f.pdf , July 2016

Lessons identified and learned

Mandate M/509 had a strong legislative and political background. With PPE being identified as an element of the 'Lead Market Initiative' there was a political and economic motivation driving the PI. Involvement of relevant stakeholder groups as e. g. the European Technology Platform for the Future of Textiles and Clothing and FP7 research projects in the early phase of the initiative assured an effective bottom-up method when it comes to the details of the work programme. The actual needs of suppliers and end users have been considered. A step-by-step approach based on a 'Lead Market Initiative' supporting an 'Action Plan for Protective Textiles' and leading to M/509 as a standardisation request as can be seen in Figure 2 led to a final report on M/509 with a work programme and a number of proposals for standardisation deliverables. Recommendations made in the final report concerned different players in standardisation as e.g. TCs, working groups, the sector forum and research institutes. This together with the number of different stakeholders from areas like safety, clothing, technology, IT and privacy leads to a complex and time-consuming work process. The recommendations mentioned in the final report were also more user-oriented compared to the product-oriented work done in the different TCs to that point. Thus an intensified user involvement is necessary and supported.

Currently the attempt to create a new horizontal TCs for PPE aspects is ongoing. There seems to be a strong discussion about the strategy and scope of such a TC which certainly might result in an efficient, determined work programme. The TC is supposed to work as a linking element between various relevant other TCs and shall especially integrate the end user needs. Additionally a close cooperation and communication with relevant ISO TCs is envisaged.

Generally it was mentioned that the whole programme enhanced the visibility and interest of and in the PPE sector which was an objective of the LMI from the beginning. A lot of experts that contributed to the findings of the final report on M/509 are still active in the implementation of the recommendations meaning a positive momentum and a greater stakeholder interest has been generated.

Even though it seems that an important and good structuring process is still going on in the field, it needs to be mentioned that 2.5 years after publishing the final report on M/509 and more than four years after M/509 was issued, no fundamental standardisation deliverables have been produced so far. In terms of the 'Lead Market Initiative', which was initiated in 2007/2008, time is crucial in order to gain the envisaged competitive advantages. The fact that mandate M/509 did not set a clear time frame might play a role here.

2.1.2.3 Mandate M/530 – Standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management

Preparation phase

The motivation for mandate M/530 arose from different initiatives and communications. These go back to 1995. The chronology of these predecessor initiatives is as follows:

- (1995) The Data Protection Directive 95/46/EC sets out a range of obligations to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.³⁸
- (2001) The Data Protection Regulation (EC) No 45/2001 has the objectives to protect the fundamental rights and freedoms of natural persons, to assure the free flow of personal data and to establish the European Data Protection Supervisor.³⁹
- (2002) ePrivacy Directive 2002/58/EC refers to privacy and electronic communications.⁴⁰

³⁸ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> , July 2016

³⁹ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF> , July 2016

- (2011) Joint Cyber Security Coordination Group (CSCG) established by CEN, CENELEC and ETSI to provide strategic advice on standardisation in the field of IT security, Network and Information Security and Cyber Security.⁴¹
- (2011) 2011/C 349/04 COMMISSION DECISION of 28 November 2011 for setting up the European multi-stakeholder platform on ICT standardisation, which is an advisory expert group on all matters related to European ICT standardisation.⁴²
- (2012) The Charter of Fundamental Rights of the EU enshrines in Article 7 privacy and recognises in Article 8 the right to the protection of personal data.⁴³
- (2013) JOIN/2013/0001 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.⁴⁴
- (2013) Annual EU work programme for European standardisation includes a standardisation request for supporting the implementation of privacy management standards.⁴⁵
- (2014) MEMO/14/186 Progress on EU data protection reform now irreversible following European Parliament vote.⁴⁶
- (2014) CSCG White Paper No. 01 'Recommendations for a Strategy on European Cyber Security Standardisation' as response to the Cybersecurity Strategy JOIN/2013/0001.⁴⁷

One of the triggers for the development of the mandate has been the work of the CSCG. The CSCG was initially a Coordination Group of the ESOs and was established in 2011 by decision of the Technical Boards of them, following a proposal from DIN to create an advisory group on Cyber Security. Its task was to coordinate the standardisation activities amongst the ESOs and to give advice on future standardisation activities on cyber security (incl. the fields of IT-security as well as prevention and detection of cyber-crime) to the technical steering committees of CEN, CENELEC and ETSI. Since these standardisation activities take place in many different standards committees and working groups, a harmonization and coordination among CEN, CENELEC and ETSI was needed to positively influence the progress and the results of these standardisation efforts. Among other things the CSCG strived to analyse existing European and international standards for cyber security, to define joint European requirements for European and international standardisation for cyber security; to suggest a European roadmap on the standardisation of cyber security taking into account EU Commission mandates as appropriate; and to interact with EU institutions and other international standards developing organisations (e. g. European multi-stakeholder platform on ICT standardisation, ISO, IEC, and from the US) with regard to standardisation in the field of cyber security. The secretary of the CSCG is provided by DIN.

One of the initiatives of the CSCG was the development of White Paper No. 01 'Recommendations for a Strategy on European Cyber Security Standardisation' published in February 2014. The paper has given nine recommendations for cyber security standardisation in the European Union with regard to governance, harmonisation and global dimension. Afterwards, in April 2014, representatives of DIN, CEN and CENELEC, ETSI and CSCG discussed the role of standards in support of the EU Cybersecurity Strategy with the Vice-President of the EC responsible for the Digital Agenda. During this meeting, the three ESOs presented their latest proposals regarding how to maximize the positive contribution that standards can make to enhancing internet security and

⁴⁰ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML> , July 2016

⁴¹ See e. g. <http://www.din.de/go/cscg> , July 2016

⁴² See <https://ec.europa.eu/digital-single-market/european-multi-stakeholder-platform-ict-standardisation> , July 2016

⁴³ See <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT> , July 2016

⁴⁴ See <http://www.ipex.eu/IPEXL-WEB/dossier/document/JOIN20130001.do> , July 2016

⁴⁵ See <http://ec.europa.eu/transparency/regdoc/rep/1/2013/EN/1-2013-561-EN-F1-1.Pdf> , July 2016

⁴⁶ See http://europa.eu/rapid/press-release_MEMO-14-186_fr.htm , July 2016

⁴⁷ See <http://www.din.de/blob/61520/377b6def0b8679a61c0252b5d1930c52/cscg-white-paper-data.pdf> , July 2016

protecting personal data, and thus to support the successful implementation of the EU Cyber security Strategy. The presented recommendations of the CSCG underline inter alia the importance of cyber security standardisation for the protection of personal data and the benefits of harmonized cyber security standards. The ESOs are calling for a coherent framework for the governance of cyber security standardisation, within the context of EU Regulation 1025/2012 on European standardisation to address these objectives.⁴⁸

Thus it can be concluded that the initiation of the mandate M/530 arose from the above mentioned regulations, communications and other documents. The formal initiation of this mandate is mentioned in the Commission Implementing Decision of 20 January 2015⁴⁹, where the ESOs are requested to initiate standardisation activities for the privacy and personal data protection management.

In 2016 additional influencing initiatives and documents are:

- NIS directive on security of network and information systems,⁵⁰
- report of the European Cybersecurity Industrial Leaders,⁵¹ and
- activities of the European Data Protection Supervisor.⁵²

The objectives of the mandate were "to develop European standards, which shall cover the following aspects:

- i. How to address and manage privacy and personal data protection issues during the design and development and the production and service provision processes of security technologies and services, allowing manufacturers and service providers to develop, implement and execute a widely recognised 'Privacy by Design' (PbD) approach in their processes; and
- ii. European standards addressed to the manufacturers and service providers when specifying the privacy and personal data protection management processes with an explanation how to realise them, including descriptions of the necessary roles, tasks, documentation, hardware and software requirements, and templates to be used when applying the requested standard(s)."⁵³

Besides the European standards the ESOs were asked to provide European standardisation deliverables which should give practical guidance for the requested European standards and thus on the implementation of privacy and personal data protection management. These guidelines should detail different aspects, such as a clear definition of security services and technologies; general information on the privacy and personal data protection management process as well as on related company staff; development of related policies at the level of manufacturers and service providers as well as documentation actions.⁵⁴

The ESOs were asked to inform the EC about the acceptance of the request within a month after receiving it. If one of the ESOs decided to answer the request with a conditional acceptance it would have been considered by the EC as a refusal. When the standardisation request was not accepted by any of the ESOs it would have been expired three months after notifying the ESOs.

Via mandate the EC asked the ESOs to develop European standards for privacy and personal data protection management. These shall fulfil several requirements, such as compatibility with EN ISO 9001 standard for supporting the integration of privacy and personal data protection management as an integral part of the quality management; a clear definition for security products and services; specific recommendations and guidelines for

⁴⁸ See http://www.cencenelec.eu/News/Press_Releases/Pages/PR-2014-04.aspx, July 2016

⁴⁹ See <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548>, July 2016

⁵⁰ See <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>, July 2016

⁵¹ See <https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders>, July 2016

⁵² See <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/cache/offonce?lang=en>, July 2016

⁵³ See <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548>, July 2016

⁵⁴ See <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548>, July 2016

the security sector, especially for manufacturers and service providers; taking into account existing standards (like ISO/IEC 27001 and ISO/IEC 27002, as well as on risk management) and current standardisation work; and using existing specifications as well as proven practices and approaches (like European privacy risk management methodologies or the 'privacy in design' approach).⁵⁵

The mandate also defined requirements for the standardisation work with regard to project planning and reporting. For this reason the ESOs were asked to send within 10 months after the notification of the mandate a joint work plan and a joint preliminary work programme indicating all requested work items, technical bodies and a tentative timetable. Afterwards the EC would give the ESOs within a month an answer to the work programme mentioning the work items to be included in the mandated work programme including any priorities. During the standardisation work the ESOs shall consult the European Data Protection Supervisor regarding the references to privacy by design. The first annual report had to be submitted to the EC in May 2016 and the final report is due for April 2019. The requested deliverables are due in January 2019.⁵⁶

Implementation phase

The mandate will be executed by CEN/CENELEC and ETSI separately through two different TCs.

Since the CSCG has mainly an advising function, the response to mandates such as M/530 has to come from a Working Group or TC. Standardisation deliverables cannot be developed by the CSCG. Therefore the CEN-CENELEC Joint Working Group (JWG) 8 'Privacy management in products and services' is responsible for responding to mandate M/530 for CEN and CENELEC. JWG 8 was created in 2014 to provide the response to the new EC standardisation request on 'Privacy management in the design and development and in the production and service provision processes of security technologies' and aims at the implementation of Privacy-by-design principles for security technologies and/or services lifecycle. The French standardisation organisation AFNOR is providing the secretary of JWG 8. The first task of the JWG was to define a work programme consisting of standards and guidance documents on how to plan, implement, control and revise a management process appropriately addressing privacy needs and requirements in each step of the design, development and production of security technologies or provision of services.⁵⁷ After a phase of preparation, the work programme of the JWG was approved in June 2016 by its members.

At ETSI the Technical Body CYBER is responsible for all related work to the mandate M/530.⁵⁸ CYBER was established in March 2014 as a new TC on cyber security to address the growing demands for standards in this field.⁵⁹ Several work items and standards have already been developed in relation to mandate M/530, such as identity management and naming schema protection mechanisms; mechanisms for privacy assurance and verification; Global Cyber Security Ecosystem; structured threat information sharing.⁶⁰ In November 2015 ETSI has submitted its work programme to the EC. The programme proposes the development of a set of standards to manage privacy and personal data protection aspects from the different stages (design, development, production and provision) of security technologies and services, and includes an ETSI Technical Report on the basic requirements for privacy management.⁶¹

The work on the mandate is still in progress by both involved TCs. Figure 3 provides an overview on the chronology of main actions regarding M/530.

⁵⁵ See <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548>, July 2016

⁵⁶ See <http://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX:52015SC0301>, July 2016

⁵⁷ See <http://www.cencenelec.eu/STANDARDS/SECTORS/DEFENCESECURITYPRIVACY/PRIVACY/Pages/default.aspx>, July 2016

⁵⁸ See <https://portal.etsi.org/tb.aspx?TBID=824&subTB=824#5068-home>, July 2016

⁵⁹ See <http://www.etsi.org/news-events/news/769-2014-03-etsi-to-develop-european-standards-for-cybersecurity>, July 2016

⁶⁰ See the [link](#), July 2016

⁶¹ See <https://portal.etsi.org/TBSiteMap/CYBER/ActivityReport.aspx>, July 2016



Figure 3: Chronology of actions linked to mandate M/530

Lessons identified and learned

Within the preparation and implementation phase a positive example of collaboration between the ESOs and the EC can be seen. With Directive 95/46/EC a legislative framework was set in 1995. In the beginning of the 21st century the cyber threat and need for privacy and personal data protection management came in focus. The ESOs built up the CSCG which prepared a white paper recommending several standardisation activities. Mandate M/530, which has been published afterwards, took up essential elements of the discussion between representatives from the EC by various DG's and experts from the standardization world within the CSCG. Sharing of information and commitment to a common understanding of future challenges enhance chances of successful mandating. Since the perspective of the ESOs and its stakeholder communities could be considered from the very beginning, market acceptance can be considered more precisely when developing mandates. Due to the detailed timeframe given by the EC the envisaged work programmes have been submitted by the ESOs and the standardisation work has already started.

2.1.3 International civil programming initiatives

Internationally the United Nations (UN) is apparently the most active organisation when it comes to PIs in general. Most actions and recommendations coming from the UN and its offices are concerned with aspects of international law, human rights and international cooperation. Unlike the EC the UN does not have a strong link to any standardisation organisation as e.g. the International Standardisation Organisation (ISO). Hence, the UN does not issue PIs in the sense of formal requests to standardisation organisations to investigate the need for or develop particular standardisation deliverables.

However, the UN is engaged in several ISO TCs as a liaison partner:

- ISO/TC 22 – Road vehicles

- ISO/TC 37 – Terminology and other language and content resources
- ISO/TC 46 – Information and documentation
- ISO/TC 51 – Pallets for unit load method of materials handling
- ISO/TC 104 – Freight containers
- ISO/TC 122 – Packaging
- ISO/TC 154 – Processes, data elements and documents in commerce, industry and administration
- ISO/TC 211 – Geographic information/Geomatics
- ISO/PC 252 – Natural gas fuelling stations for vehicles

Contributions by the UN are mostly connected to sustainability aspects deriving from the UN's agenda. In this light the website of the UN states: "The UN system works in a variety of ways to promote economic and social goals. The mandates of the specialized agencies⁶² cover virtually all areas of economic and social endeavour. The agencies provide technical assistance and other forms of practical help to countries around the world. In cooperation with the UN, they help formulate policies, set standards and guidelines, foster support and mobilize funds."⁶³

One specific approach which involves measures respectively recommendations regarding standardisation taken by the UN is the 'Sendai Framework for Disaster Risk Reduction 2015 – 2030'. It was adopted by UN Member States in Sendai, Japan, on 18th March 2015 at the World Conference on Disaster Risk Reduction (WCDRR) and articulates "the need for improved understanding of disaster risk in all its dimensions [...]"⁶⁴

The high level objective is the substantial reduction of "disaster risk and losses in lives, livelihoods and health and in the economic, physical, social, cultural and environmental assets of persons, businesses, communities and countries."⁶⁴ In terms of that the Sendai Framework is set out with seven targets and four priorities for action to reach the goal of disaster risk reduction. Particularly interesting is that the Sendai Framework suggests both the development and the revision or improvement of standards as necessary actions in the course of disaster risk reduction in its four priorities. There is no direct involvement of SDOs in the work programme of the initiative but e.g. ISO/TC 292 'Security and resilience' established a task force in order to seek opportunities for cooperation in the area of disaster risk reduction and facilitate the implementation of frameworks as e.g. the 'Sendai Framework. However, since the Sendai Framework does not request any SDO neither any other institution to investigate the need for respectively the development of specific standards it is not considered a PI within the scope of this report.

Besides the UN, further organisations as e.g. other regional standardisation organisation across the globe have been investigated for PIs similar to the European mandates. In particular the African Organisation for Standardisation⁶⁵, the Arab Industrial Development and Mining Organisation⁶⁶, the Pacific Area Standards Congress⁶⁷, Pan American Standards Commission⁶⁸, the EuroAsian Interstate Council for Standardisation, Metrology and Certification⁶⁹ and the ASEAN Consultative Committee on Standards and Quality⁷⁰ have been looked into. No such things as PIs regarding standardisation or any related activities could in fact be identified. It

⁶² In work package 2 of the ResiStand project those UN specialised agencies as e.g. the International Maritime Organisation (IMO), the World Meteorological Organisation (WMO) or the International Civil Aviation Organisation (ICAO) are going to be investigated in regards to their standardisation activities.

⁶³ <http://www.un.org/en/development/other/overview.shtml>, May 2016

⁶⁴ United Nations Office for Disaster Risk Reduction (UNISDR): Sendai Framework for Disaster Risk Reduction 2015 – 2030 (Sendai). Geneva 2015

⁶⁵ <http://www.arso-oran.org/>, May 2016

⁶⁶ <http://www.aidmo.org/index.php?lang=en>, May 2016

⁶⁷ <http://www.pascnet.org/>, May 2016

⁶⁸ <http://www.copant.org/index.php/en/>, May 2016

⁶⁹ http://www.easc.org.by/english/mgs_org_en.php, May 2016

⁷⁰ <http://asean.org/asean-economic-community/sectoral-bodies-under-the-purview-of-aem/standards-and-conformance/>, May 2016

is concluded that regional or trans-national standardisation is not very common or at least not as pronounced in other regions as it is in the European Union.

2.2 *Military standardisation*

Standardisation plays an important role in the military domain and has been conducted in the context of NATO since decades. Therefore, a broad range of experience on how to identify, initiate, implement and follow-up standardisation needs and actions has been gained in NATO and their allied nations. Whereas military standardisation remains out of scope of H2020 activities, the knowledge and experience gained by the military can be of added value for the civil domain of EU security as long as the knowledge and experience are transferable into civil domain. On the homepage of NATO the following information can be retrieved regarding the importance of standardization for NATO: "It is highlighted by NATO that the ability to work together is more important than ever for the Alliance. States need to share a common set of standards, especially among military forces, to carry out multinational operations. By helping to achieve interoperability among NATO's forces, and partners, standardisation allows for more efficient use of resources and thus enhances the Alliance's operational effectiveness."

NATO standardisation is the development and implementation of concepts, doctrines and procedures to achieve and maintain the required levels of compatibility, interchangeability or commonality needed to achieve interoperability in the operational, procedural, material and administrative fields. This includes for example a common doctrine for planning a campaign, standard procedures for transferring supplies between ships at sea, and interoperable material such as fuel connections at airfields. It permits NATO countries to work together, as well as with their partners, preventing duplication and promoting better use of economic resources."⁷¹

2.2.1 *NATO standardisation*

Structure of NATO standardisation

The NATO Standardization Office (NSO⁷²) assists NATO's Military Committee in developing military operational standards. The NSO initiates, coordinates, publishes and manages a database of NATO standardisation documents and supports and administers NATO standardisation activities, which are conducted under the authority of the Committee for Standardisation (CS). In the CS, representatives from all NATO countries are represented, and CS is responsible for standardisation policy and management within the Alliance. The Committee contributes to interoperable and cost-effective capabilities and it reports directly to the North Atlantic Council (NAC). NATO senior committees which are authorized to develop and maintain NATO standards are called "Tasking Authorities" (TA).

Standardisation requirements can be established in two ways. The first is the top-down process, where standardisation issues are addressed through the NATO Defence Planning Process (NDPP). Strategic commands identifying standardisation requirements and the NSO execute the task. The second possibility is the bottom-up process, where nations or NATO commands report standardisation need and file a proposal to NSO (see Figure 4). The standardisation bodies of NATO are described in more detail in references^{73 74}.

⁷¹ http://www.nato.int/cps/en/natohq/topics_69269.htm

⁷² <http://nso.nato.int/nso/SOSite/default.html>

⁷³ Aksit, C. The Importance of NATO standardisation. Defence Procurement International, 2012. Page 1-3.

⁷⁴ AAP-03. Production, maintenance and management of NATO standardisation documents. Edition J, version 3. Published by the NATO STANDARDIZATION OFFICE (NSO)



Figure 4: Procedures for development of standards in NATO (modified from Cihangir Aksit)

NATO standards

A standardization agreement (STANAG) is a NATO standardisation document that specifies the agreement of member nations to implement standards, in whole or in part, with or without reservation, in order to meet an interoperability requirement⁷⁵. A STANAG must respond to an interoperability requirement and is subject to ratification by nations and nations shall provide NATO with a feedback on the implementation status. A STANAG specifies the agreement of member nations to implement standards. A STANREC (Standardization recommendations) is voluntary for the nations to follow and is not related to interoperability requirements. A ratification process is not run and the standards are approved by TAs. Other standards are Allied standards, which are NATO and non-NATO standards (civil and military) standards. The NATO Policy for standardisation states that the Alliance will use suitable civil standards to the maximum practicable extent and only when no applicable civil standard is available, a NATO standard will be developed.

NATO has established Technical Cooperation Agreements (TACs) with civil SDOs to promote cooperation in the field of standardisation of mutual interest. The NATO STANAG 2345 (Military workplaces-force health protection regarding personnel exposure to electric, magnetic and electromagnetic fields, 0 HZ TO 300 GHZ) has been developed into a civil standard (C95.1-2345-2014 - IEEE Standard for Military Workplaces)⁷⁶ based on the STANAG.

Lessons identified and learned

In NATO standardisation is regarded as important tool to ensure interoperability among NATO forces and standardisation is therefore highly prioritized. NATO has their own standardisation office called NSO that is responsible for the NATO standardisation activities and coordinates the process and cooperation with the nations. It is a national responsibility to implement a STANAG. Either a top down or a bottom up process can be used for proposing new standardisation activities.

2.2.2 National military standardisation

Example Germany

In the German defence sector mainly civil standards published by DIN, the ESOs and ISO/IEC are utilised to develop and procure defence technological products. In case civil standards are not applicable to military requirements the common practice is trying to integrate these requirements in the existing civil standards in

⁷⁵ http://www.nato.int/cps/en/natohq/topics_69269.htm

⁷⁶ <https://standards.ieee.org/findstds/standard/C95.1-2345-2014.html>

order to become applicable for military purposes. Doing so the process of civil standardisation stated in DIN's, the ESOs' and ISO/IECs' regulations is followed and the respective defence-related stakeholders participate regularly in the development and adaption of standardisation deliverables. Only if defence-related aspects cannot be considered in civil standards, experts from the defence sector are collaborating separately to develop suitable defence equipment standards.⁷⁷ Nevertheless this is done in compliance with the regulations of the civil defence-technological TCs at DIN. Those standards are to be withdrawn if appropriate civil standards which meet the specific defence-related requirements are published.⁷⁸

Concluding, there are defence-related standardisation activities besides the regular civil standardisation in Germany that are supporting the military sector. These are conducted on basis of a yearly renewed contract between the German Federal Ministry of Defence (BMVg) and the German Institute for Standardisation (DIN). The BMVg provides a defined budget and expected performance specifications. The Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw) which is under the authority of BMVg is responsible for decisions about which defence equipment standards are to be developed, adjusted or withdrawn on national level. Comments of other stakeholders as e.g. industry are considered but not decisive. DIN has the function of an administrative office for the context of military standardisation. In practice BAAINBw sets specific requirements about standards to be developed in defined areas and DIN leads the process of developing these standards with participation of relevant stakeholders, equivalent to the regular civil standardisation.

Lessons identified and learned

In Germany the exclusive national defence equipment standardisation is regulated within a contract between DIN and the respective Federal Ministry. The contract builds the framework in which clear requirements are set by the customer which is the main stakeholder at the same time. A clear budget for standardisation activities is given as well. Decisions about what aspects are going to be standardised are primarily made by the Federal Ministry. Thus the openness of the standardisation process is limited. Since at the end all relevant stakeholders can be fairly seen as suppliers to the Federal Ministry, the process might be appropriate in this field. Based on the contract between DIN and the Federal Ministry this initiative can be interpreted as a PI.

2.2.3 Hybrid standards and M/512

2.2.3.1 Hybrid standards

The defence sector uses either civil, dual-use or specific military standards. Efforts are made to exploit civil-military synergies in the area of research and development. The EC has, in cooperation with the European Defence Agency (EDA), recommended the development of so-called hybrid standards. These are standards intended to apply to both the civilian security sector and the defence sector. The harmonisation of applied defence standards in Europe is a key enabler for interoperability of materiel used by European forces. The ESOs have created a Defence Standardisation group (DCSG) with the aim of facilitating cooperation between military and civil standardisation communities in Europe⁷⁹. EDA in cooperation with CEN-CENELEC-ETSI/DCSG has developed a new procedure for developing hybrid standards. DCSG will continue to promote collaboration among all the relevant stakeholders, including the EC, EDA and the NATO NSO office.

The EC has committed itself to promoting the development of dual-use or 'Hybrid Standards' for products which can have both military and civilian applications. The need to reinforce the competitiveness of the defence industry has been highlighted in the framework of the Europe 2020 Strategy in its communication on the

⁷⁷ "Verteidigungsgeräte-Normen" (VG-Normen, defence equipment norms), "Werkstoffleistungsblätter" (WL-Blätter, material performance sheets)

⁷⁸ http://www.baainbw.de/portal/a/baain/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pMTEzDy9stSi9MSkVL28_KLc1Lwy_YJsROUAGVYYjQ!!/, July 2016

⁷⁹ CEN/CENELEC Work Programme 2016.

defence and security sector⁸⁰. The Commission is cooperating with EDA for the development of these standards. This must be done in agreement with Member States taking full account of national sovereignty and ensuring no duplication with NATO. The DSCG and MSG (Material standardization group) at EDA work together for writing a common procedure for developing the security/ defence standards which will fix the role and responsibilities of each European defence stakeholders.

EDA maintains the tools EDSIS (European Defence Standardization Information System) and EDSTAR (European Defence Standards Reference System) to support harmonisation and standardisation activities and projects. The EDSTAR database is listing military standards and best practice recommendations for the specific technical domains.

Software Defined Radio (SDR) was one of the first areas to be identified as potential areas for hybrid standards. A standardization mandate for reconfigurable radio systems was published by the EC (M/512), and a SDR standardisation roadmap was prepared by EDA. The mandate has been sent to ETSI for further work and development. The detailed analysis of M/512 is provided in the next clause.

Other proposals for hybrid standards, even though they seem to have not been further developed so far, are:⁸¹

- RPAS: The airworthiness requirements for Remotely Piloted Aircraft Systems (RPAS) have been proposed. RPAS have demonstrated their importance in recent military operations, particularly for surveillance and information gathering. However RPAS can also offer a wide range of civil applications such as infrastructure surveillance, firefighting, disaster or environmental monitoring, as well as border control and management.
- A proposal addressing hybrid tyres (bulletproof tyres that comply with FINABEL⁸² standards) was submitted by Germany and was accepted and included in EDA's hybrid standardisation programme.⁸³ The aim of the hybrid standards is to establish modern test procedures in the form of a European Standard (EN).
- Slovenia has submitted a proposal for protective shields that are used, for instance, by the police but are also procured by individual European armed forces such as the Bundeswehr from Germany.
- A British proposal was also presented on the topic "Measurement of Impulse Noise from Military Weapons, Explosives and Pyrotechnics (MWEP)".

2.2.3.2 *Mandate M/512 – M/512 Standardisation mandate to CEN, CENELEC and ETSI for Reconfigurable Radio System*

Preparation phase

The motivation for the development of Mandate M/512⁸⁴ was that Reconfigurable Radio Systems (RRS) are expected to become important drivers for the evolution of wireless communications and are going to bring substantial benefits and a better utilisation of the radio frequency spectrum, thereby helping to mitigate the spectrum scarcity problem. RRS, and in particular Software Defined Radio (SDR) and Cognitive Radio (CR) technologies have been investigated in the commercial domain and in the public safety and military domains. Each of these domains has specific operational and technical requirements, and a consistent approach should bring benefits for all areas. The initiator for the mandate was EU and EDA drafted the mandate in co-operation with ESSOR⁸⁵ nations and Germany. Although there are potentially a number of synergies between commercial, civil security and military domain, there are also discussions regarding what is really feasible and what is not and

⁸⁰ COM(2013) 542

⁸¹ Because these topics are no further developed, they could be further analysed in the context of this document

⁸² The Finabel (*France, Italy, Netherlands, Germany/Allemagne, Belgium, Luxembourg*) Coordination Committee is a Land Forces organisation comprised of 21 Member States of the European Union to promote interoperability between its Members, cf. www.finabel.org

⁸³ Information from Peter Hecker, Head of Technical Group 2.4 at DIN

⁸⁴ <http://www.etsi.org/images/files/ECMandates/m512.pdf>

⁸⁵ ESSOR Nations: Finland, France, Italy, Poland, Spain and Sweden

ETSI (TC RRS)⁸⁶ is currently investigating (under EC mandate M/512) how reconfigurable radio systems can help to achieve those same synergies. Reconfigurable radio technologies are also under investigation in the military domain where demand for military communications is expected to rise and therefore there is the need to maximise the use of the radio spectrum. In this regard cognitive radio is under investigation in NATO (STO) and the EDA (e.g. with the project CORASMA)⁸⁷. Cognitive radio is here expected to be complementary to SDR.

Within the civil security domain, the evolution of wireless communications in civil security should address three significant challenges:

- a) Lack of interoperability due to different technology standards and systems;
- b) Lack of broadband connectivity to support a wide range of new applications;
- c) Economic sustainability.

The provision of adequate capabilities to civil security organisations is a priority subject for citizens, National Governments and the EU. This is also highlighted by the following communications and decisions:

- Council Decision 2007/162/EC,
- Council Decision 2008/615/JHA of 23 June 2008
- COM (2008) 130 Communication from the Commission to the European Parliament and the Council on reinforcing the Union's Disaster Response Capacity, and
- COM (2010) 600 towards a stronger European disaster response: the role of civil protection and humanitarian assistance.

Within the military domain, the scope of the military standardisation of the SDR software architecture is to promote the portability of different waveforms to different SDR platforms in order to pave the way for interoperability in the military domain. The standards produced by the SDO shall fulfil all the requirements needed to be proposed as a NATO STANAG. Communications and decisions:

- US JTRS⁸⁸ programme
- Three different developments of 'SDR architectures' running in parallel: US SDR architecture, ESSOR SDR architecture and German SDR architecture

Within the commercial domain, mandate M/512 intends to stimulate standardisation to position Europe at the forefront of experimentation with RRS technologies in the area of pre-commercial and commercial applications. This should make it possible to exploit the opportunities for use of RRS technologies in a timely way, supported by market demand and by adaptations in the regulatory framework. There are lots of ongoing research projects to develop technology for cognitive radio system able to operate efficient in multiple different frequency bands and several EU projects (FP5, FP6) have studied SDR radio systems.

The mandate M/512 identifies an approach and a number of issues where standardisation should enable the development and use of RRS technologies, in particular SDR technologies, in Europe. The objectives of the M/512 mandate are⁸⁹:

- identify/define items to standardize;
- identify/define the global framework of the standardization including interfaces (e.g. NATO, WINNF, US JTRS) and policies;

⁸⁶ <https://portal.etsi.org/TBSiteMap/rrs/rrstor>

⁸⁷ <http://perso.telecom-paristech.fr/~hachem/peyresq2013/lemartret.pdf>

EDA ad hoc B program. CORASMA project cognitive radio for dynamic Spectrum management contract N B-781-IAP4-GC

⁸⁸ US JTRS: Joint Tactical Radio System

⁸⁹ <http://www.etsi.org/images/files/ECMandates/m512.pdf>

- identify/define harmonized Rules and Procedures to achieve the SDR SW Architecture Military Standard taking into account the MODs' requirement to maintain control on the process;
- address any financial resources associated with tasks' accomplishment.

The expected impact of the mandate is to create and promote an international standard defined by European nations and USA. EU drafted the M/512 in 2011 together with EDA in co-operation with ESSOR nations and Germany (government and industry). The EC requested the SDOs (ETSI) to execute the mandate, and to develop harmonised standards, and the request was formally accepted by ETSI in May 2013. A SDR standardization strategic guidance working group in EDA (2012) created a roadmap for the military standardisation, and the goal was to identify items to standardise and monitor the evolution of the standardisation process. According to the roadmap the standardisation phase was expected to be from 2013 to 2017 and items to standardise should be suggested and identified⁹⁰. The standardisation initiative was expected to have a big impact and be an important driver for the evolution of wireless communication including the commercial, civil and military area. However, on request from EDA, the work to develop standards in the SDR architecture for the military domain as well as SDR architecture for the civil security domain was frozen⁹¹. We have no further information about the further standardisation process in this area.

Implementation phase

Upon receiving the standardisation mandate a detailed plan for the objectives were requested and made. ETSI was requested to invite appropriate stakeholders to be involved in the standardisation work. Stakeholders were supposed to be selected; from the civil security/military domain (Ministries of Defence (MODs), EDA, FROTEX, Europol etc. In the civil sector technical reports have been published by ETSI. To our knowledge, no hybrid (military/civil) standards developed as a response to the mandate.

Lessons identified and learned

Development of hybrid standards can benefit both civil and military communities. In the civil sector technical reports have been published by ETSI in the Reconfigurable Radio Systems (RRS)⁹². We have no information about development of military or hybrid standards. Difficulties related to collaboration between civil and military domains in standardisation processes should be highlighted and possible compromises worked out.

⁹⁰ EDA Ad Hoc working group (WG) on SDR standardisation strategic guidance (SDR SSG). Carlo Zammariello, EDA 26 June, 2013.

⁹¹ EC mandate on RSS: Status of activities and the way to move forward; EC Workshop on CR standardization- Brussels, October 22nd © ETSI 2011. All rights reserved. Presented by Andrea Lorelli, ETSI Secretariat

⁹² <http://www.etsi.org/standards>

3 Analysis and review of M/487

Mandate M/487 is listed in Table 2 as one of the relevant European PIs. As this mandate is the most relevant PI for the ResiStand project, M/487 is analysed more in-depth and is included as a separate chapter.

3.1 Preparation phase of mandate M/487

3.1.1 Description of the preparation phase

Activities that led to the mandate development

Mandate M/487 was initiated by the unit “Security Research and Development” (H3), DG ENTR at the EC⁹³ in 2010. DG ENTR was responsible for R&D in the (civil) security domain, which included the goals of strengthening the competitiveness of the EU Security Industry, and facilitating cross-border collaboration of public and private “end users” in security, thus calling for improved interoperability. Several policy initiatives in security and regarding EU competitiveness⁹⁴ at that time underlined the need for accelerated European standardisation, thus also DG ENTR H3 was requested to analyse the needs and opportunities for accelerating standardisation in the security domain. However, DG ENTR lacked an overview of the situation of already existing standardisation activities or standardisation activities in being in preparation in the security domain, not least due to the cross-cutting nature of security across the industrial sectors, and the various planned, ongoing or already completed FP7 security R&D projects addressing, among other issues, standardisation needs and opportunities. So, the need was clear to get this overview first, before concrete standardisation topics could be identified and substantiated by respective standardisation mandates.

The “design process” of M/487 followed the internal rules of the EC for drafting and issuing such mandates. However, as M/487 was the first, horizontal mandate in the area of security, there was an information exchange between unit H3 and the DG ENTR unit responsible for M/415 “Programming Mandate addressed to CEN, CENELEC and ETSI to establish Space Industry Standards”, which functioned as an example for the development of M/487. The main interaction when preparing M/487 seems to have taken place in DG ENTR internally.

Content of the mandate, expected impact and conditions for execution

Mandate M/487 was issued in February 2011: a study was requested to the ESOs to analyse the current standardisation ‘landscape’ in the field of security and the development of a proposed work programme. The scope of the mandate was⁹⁵:

“This Mandate concerns the development of a work programme for the definition of European Standards and other standardisation deliverables in the area of SECURITY⁹⁶. The programme will take

⁹³ The unit “Security Research and Development” (DG Enterprise and Industry) changed to unit “Innovation and Industry for Security” (DG Migration and Home Affairs) in 2015.

⁹⁴ List of policy initiatives mentioned in M/487: ESRIF report, Communication on reaction to ESRIF, Study on Competitiveness of the EU Security Industry, Communication towards an increased contribution from standardisation to innovation in Europe, The Stockholm Programme.

⁹⁵ Mandate M/487 (2011): <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=472#>

note of all aspects linked to the different specific products, systems, procedures and protocols that should be covered by standards to assist the EU to ensure that security is better and consistently addressed in different security landscapes. This Mandate has an exclusively civil application focus.”

The overall objectives were⁹⁷:

- “To increase the harmonisation of the European security market and reduce fragmentation with the establishment 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 (taking into account the already existing) 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.”

M/487 consisted of two phases – a first “landscaping phase”, and a second phase, working out concrete standardisation needs and opportunities in selected security sectors, based on the results of Phase 1. The work plan as described in M/487⁹⁸:

- “Phase 1. CEN, CENELEC and ETSI shall provide, within 8 months of the acceptance of this Mandate the result of the preparatory study and a list of sectors for priority treatment to be agreed by the Commission services. The Commission will endeavour to review the study and select some security sectors within a further three months.
- Phase 2. CEN, CENELEC and ETSI shall provide the proposed standardisation programmes and roadmaps related to the agreed security sectors within 6 months of the acceptance of the report of Phase 1 and the Commission's selection of priority sectors, for consideration for subsequent execution in a possible future phase.”

Based on the outcomes of M/487, further mandates from the EC were expected to request standardisation in the identified “priority areas” in security (i.e. areas in particular need of accelerated standardisation), to facilitate implementation of specific standardisation work programme and thereby acceleration of standardisation in the security sector.

3.1.2 Review of the preparation phase

Top-down approach

In the case of M/487, and at that time, the approach taken by the EC to issue a Programming Mandate to the ESOs to establish security standards was probably the most suitable option available, from the point of view of the EC, as mentioned before.

⁹⁶ The security concept here includes, among others, protection against threats by terrorism, severe and organised crime, natural disasters, pandemics and major technical accidents. It excludes defence and also space technology, 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’)

⁹⁷ Mandate M/487, chapter 3

⁹⁸ Mandate M/487, paragraph 4.3

Design of mandate M/487

The “design process” of M/487 followed the internal rules of the EC for drafting and issuing such mandates, so there should not have been any “surprises” on the side of the ESOs nor other security stakeholders that the EC is heading for such an approach. Nevertheless, as it was the first time ever for this sectoral unit at DG ENTR to deal with standardisation, the experience how to deal best with it etc. still had to be gained and might have resulted in less informal interaction with the ESOs and other security stakeholders already during the set-up of M/487 as it might have been possible and maybe even advisable – though not requested by any legal provision.

M/487 gives a general guideline on what is expected and does not go into detail regarding the execution of the work. This allowed all involved parties to have discussions on the execution of the work, which served as a good basis to work out the work plans for both phases. The results of these discussions were included in the internal report on the arrangements for Phase 1, and in the quotation for Phase 2.

Time frame and resources

One aspect which might have implied the need for more interaction between the EC and the ESOs could have been the time frame, which has been set out by the EC for executing Phase 1 and Phase 2 of M/487. Phase 1, which requested a complete landscaping of the situation of standardisation in the security domain, was planned by the EC for max. 8 months, and Phase 2, which requested the development of standardisation programmes and roadmaps related to the security sectors selected based on the results of Phase 1, was set out for max. 6 months after acceptance of the Phase 1 report by the EC. Probably, both phases would have benefitted from more time (and in addition the availability of funding for Phase 1) for their execution with regard to the level of detail and comprehensiveness of the analyses undertaken, in particular when comparing these time frames with the ones of e.g. Coordination and Support Actions (CSAs) in FP7/H2020, which from the type of activity could be seen as closely linked to the programming work to be done in a Programming Mandates, and which typically run 18 – 24 months.

In general, the execution of the setting-up process of M/487 revealed neither particularities nor ineffective measures taken. However, the fact that in the end only Phase 2 of M/487 could have been financed by the EC posed a particular challenge (and resource limitation) to the execution of Phase 1, which was done by NEN on its own costs.

3.2 Implementation phases of mandate M/487

3.2.1 Description of the implementation phases

Organisation of work

CCMC, representing the ESOs, was contacted to further discuss the acceptance of the request and execution of the work. CCMC’s policy is only to coordinate such requests, but not to execute the work. For the execution of the work, member countries are involved. The most relevant European TC in the area of security is CEN/TC 391 ‘Societal and Citizen Security’. The secretariat of CEN/TC 391, which was held by NEN, was thus invited to coordinate the execution of the work (see Figure 5 for an overview).

Extensive discussions between the EC, CCMC and NEN have taken place then. One of the issues was the limited time to execute the work; but the EC insisted in keeping the time schedule as stated in M/487. Regarding the execution of the mandate work, it was agreed that:

- CEN/TC 391 would take the overall lead, while a dedicated “Mandate M/487 Working Group” would be established to prepare the Phase 1 report, including various representatives of relevant technical bodies and other groups,
- a small informal coordination group would be established, providing CEN/TC 391/WG ‘M/487’ with additional support and information as well as keeping the Technical Boards informed of the progress of the work, and
- Phase 1 was to be carried out in 2 stages. The first stage would result in a single, coordinated report, while the second stage would include a proposal for the organisation of the work for Phase 2 based on the results of the first stage.

The above points were noted in Annex 1 to BT N8625, which includes the draft resolution for the Technical Boards (BT) of CEN and CENELEC to decide on the acceptance of the mandate work as specified (see Annex 2).

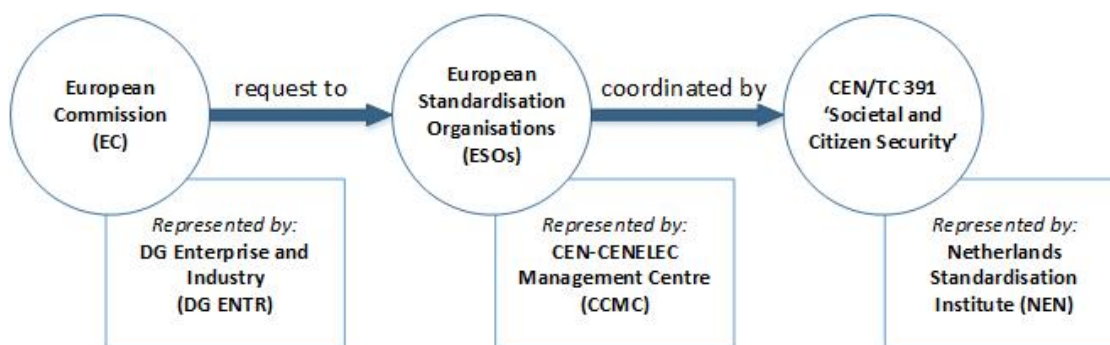


Figure 5: Involved organisations and representation

Upon acceptance of the BTs of the mandate work, overall preparations were completed. The work for Phase 1 was ready to start. A report setting out the arrangements for the execution of M/487 was presented to the EC within two months of the date of acceptance of M/487, as it was required in M/487. This report included a detailed work plan for Phase 1. Further preparations for Phase 2 could only start after obtaining the results for Phase 1. NEN, representing the secretariat of CEN/TC 391, was involved as contractor; however, no EC funding was available for Phase 1. For Phase 2 instead a “Quotation for a Grant Agreement for an Action” was submitted to the EC and accepted. The quotation included a detailed description of the work plan for Phase 2.

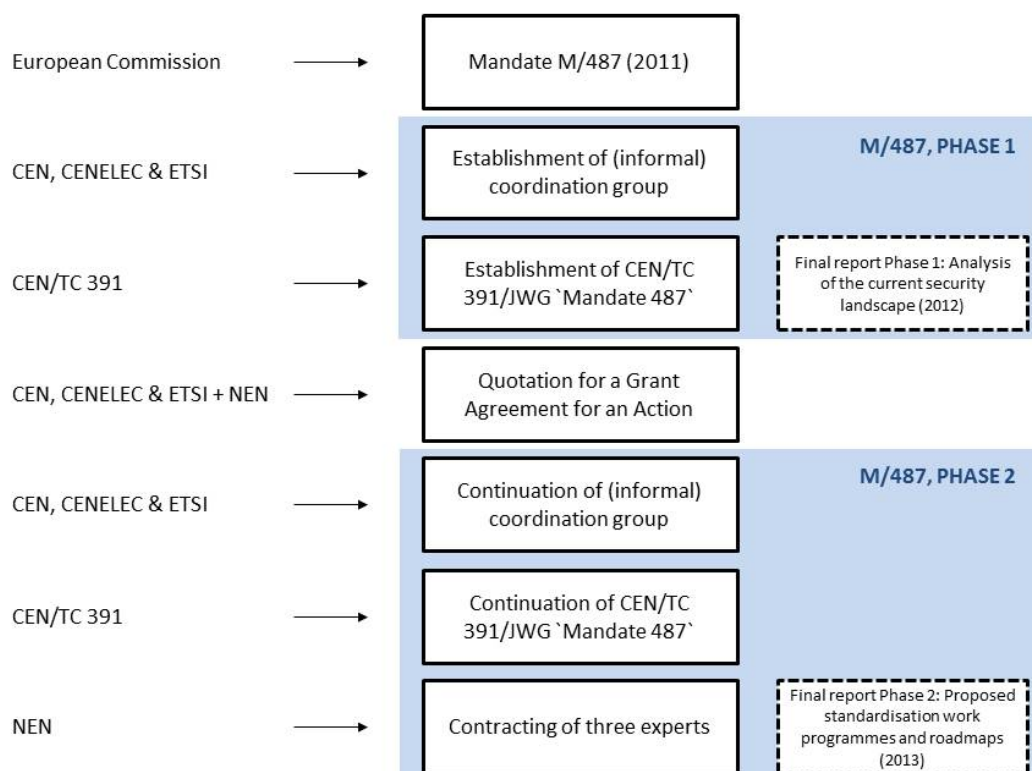


Figure 6: Timeline of actions linked to mandate M/487

Phase 1 – Preparatory study

Organisation of work

The objective of Phase 1 according to M/487 was to deliver a “preparatory study identifying the state of play in security standardisation in Europe, and list a set of [security] sectors for priority treatment, as well as the particular stakeholders needing to be involved in each of these sectors.”

The starting points for Phase 1 were the agreements based on the discussions between EC, CCMC and NEN as mentioned before. An internal report was presented to the EC setting out the arrangements for the execution of M/487 within two months of the date of acceptance of M/487. This report provided further details on the work plan. The work of Phase 1 was further divided into two stages:

- Stage 1: provide an overview of the current ‘landscape’, who is doing what, which areas might be highlighted for priority treatment, followed by an informal check by the EC, and
- Stage 2: work on a selected, small(er) number of specific subjects for more in-depth study work.

The division in two stages allowed the EC to have the initial findings at the earliest opportunity. However, as output of Phase 1, one report from the ESOs was expected.

The preparatory study in Phase 1 covered:

- analysis of national (only in the countries of CEN/TC 391 members), European and international security activities and standards,
- analysis of selected reports, communications, research projects and other written sources,
- interviews with selected stakeholders, and
- general stakeholder analysis.

As a basis for the analysis, the mandate provided a (non-exhaustive) list of areas for analysis: Security of the Citizens, Security of infrastructures and utilities, Border Security, and Restoring security and safety in case of crisis. Human factor issues, privacy concerns and identification of operator requirements for enhancing systems effectiveness should also be taken into account. ICT explicitly was not covered by the mandate with the exception of cryptography.

Two groups were formed (see Figure 7 for an overview):

1. A Joint Working Group Mandate 487 (JWG M/487) was established under the project leadership of CEN/TC 391 ‘Societal and citizen security’ to handle the response to the mandate. This ad-hoc group was open for members and technical bodies of CEN, CENELEC and ETSI, other ‘technical’ groups in the security field, bodies and organisations identified in M/487 as being relevant and interested EC services. All parties identified relevant have been approached and invited.
2. A small informal coordination group that provided the JWG with additional support, information and any guidance it might require. The coordination group consisted of the chairman and secretary of CEN/TC 391, the ETSI OCG Security group chairman, and representatives of the EC/EFTA, ETSI Secretariat and CCMC.



Figure 7: Involved organisations for the execution of M/487 Phase 1 (Source: Final report Phase 1)

Results of work in Phase 1

Desk research for the inventories was combined with in-depth interviews with stakeholders and comprehensive stakeholder surveys (national standards, FP7 projects and their findings regarding standardisation, and CEN/TC 391 members). Stakeholder involvement was further encouraged via external stakeholder meetings⁹⁹ as well as via the JWG¹⁰⁰. More stakeholder involvement and detailed stakeholder analysis was not possible due to the limited amount of time and own resources available. The report resulted in a list of six priority recommendations¹⁰¹:

- border security,
- aviation security,
- Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE),
- crisis management and civil protection,
- personal data protection, and
- general coordination of European security standardisation.

The main work was done by the secretariat (NEN), while being supported by the coordination group and input provided via the JWG and stakeholders meetings. Prior to finalisation of the Phase 1 report, the draft report was circulated to the involved stakeholders for comments. The final report was presented to CCMC for further submission to the EC. Upon submission of the report, the EC was given three months to review the study and select the priority areas for Phase 2.

The foreseen duration of Phase 1 according to the mandate was eight months; in practice it run nine months from May 2011 to January 2012. The Phase 1 final report was submitted to the EC in March 2012.

Phase 2 – Standardisation programmes and roadmaps

Organisation of work

The objective of Phase 2 according to M/487 was that “for each [selected] sector, the specific standardisation needs will be identified and comprehensive standardisation programmes with suitable and realistic roadmaps shall be prepared”.

⁹⁹ Two stakeholder meetings were held: the first meeting on 29 September 2011 (49 participants) and the second meeting on 2 March 2012 (21 participants).

¹⁰⁰ The JWG met in conjunction with CEN/TC 391 meeting on 24 October 2011. During this meeting the progress of the mandate was discussed, the approach for the inventory on standards and priorities, and the criteria for priority treatment. The JWG also provided comments to the draft report.

¹⁰¹ Final report Phase 1 “Analysis of the current security landscape” (2012)

After review of the Phase 1 report, the EC selected three priority areas to be further worked out in Phase 2, which were communicated in the Security Industrial Policy¹⁰²:

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

The execution of Phase 2 was based on a quotation, applying for a “Grant Agreement for an Action”. The quotation was prepared by NEN and CCMC, and included a detailed plan on the execution of Phase 2 in the required six months, amongst others a detailed description of all the tasks, and an overview of the involved parties and their roles.

For Phase 2, for each of the three sectors, the work was carried out in three stages:

- Stage 1: Identification of existing standards, recommended practices and standardisation needs.
- Stage 2: Development of standardisation programmes with roadmaps.
- Stage 3: Communication of the results.

The coordination group and JWG as established in Phase 1 were maintained. Due to time limitations and lack of expertise within the standardisation bodies, three external experts were involved to support the work in the three security areas¹⁰³. The role of the experts was to understand the stakeholders’ needs and gain consensus in the content of the work programme. The experts were therefore tasked to carry out a document study and several interviews with key stakeholders, lead the workshops and draft a suitable and realistic work programmes accordingly. The experts also joined the coordination group. The experts were subcontracted; selection procedures as specified by the EC applied.

The experts supported NEN focused on the content of the project, while NEN took care of the project management, the organisation of workshops, reporting, and the contact with the JWG and coordination group. Several meetings with the JWG (in conjunction with CEN/TC 391 meetings) were organised. The coordination group had more frequent contact via different means.

Results of work in Phase 2

To ensure as much involvement of stakeholders as possible, the main focus of Phase 2 was to organise three workshops, one workshop for each priority area¹⁰⁴. In preparation of the workshops, the experts gathered information by carrying out a document study and interviewing several key stakeholders. Also, prior to the workshops, standardisation proposals from stakeholders were collected and categorised, which were used as discussion points for the workshops. In this way, stakeholders that could not participate to the workshops were still able to provide input for the discussions.

The workshops were open for all interested stakeholders. Each of the experts led the respective workshop, supported by the coordination group. More than 300 proposals were discussed and prioritized by more than 200 participants in total. There was a balanced participation of stakeholders in this process, coming from security industry (including SMEs), research institutes, end-users, consultants, standard experts and local, national and

¹⁰² Communication from the Commission to the European Parliament, the Council and the European economic and social committee, COM(2012) 417 final: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF>

¹⁰³ The experts involved in Phase 2 are: Chris Hurrey (Border Security), Alain Coursaget (Crisis Management and civil protection) and Eelco Dykstra (CBRNE)

¹⁰⁴ The workshops were held on: Border security on 4 – 5 April 2013 (Frontex, Warsaw, Poland), Crisis management and civil protection on 9 - 10 April 2013 (City of Edinburgh, Edinburgh, United Kingdom), CBRNE on 11 – 12 April 2013 (JRC, Ispra, Italy).

international authorities. The workshops were evaluated and the feedback showed that the participants appreciated the way this process was organized.

The results of the document study, interviews with key stakeholders, and workshops formed the basis for the standardisation programmes and roadmaps. The high level standardisation roadmaps can be found in Figure 8, Figure 9, and Figure 10. The prioritised standardisation proposals can be found in the report¹⁰⁵.

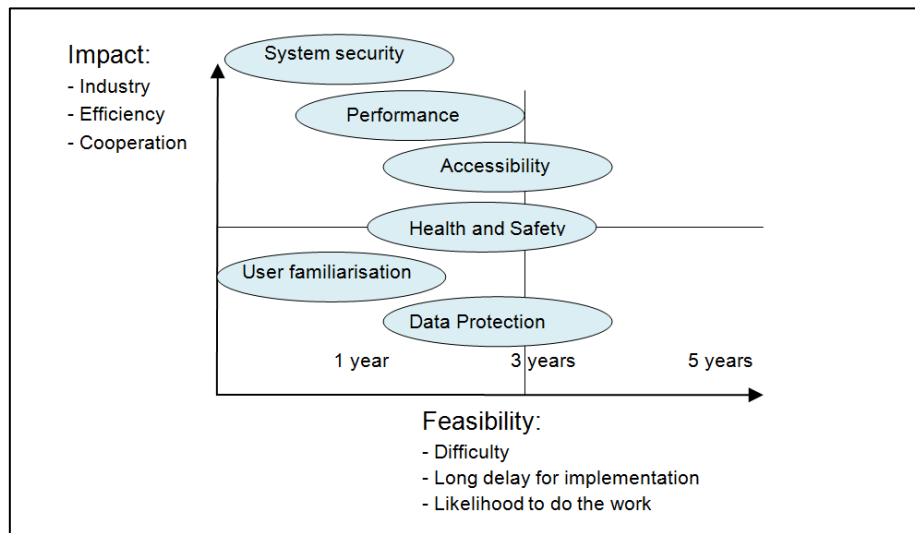


Figure 8: High level standardisation roadmap for border security (Source: Final report Phase 2)

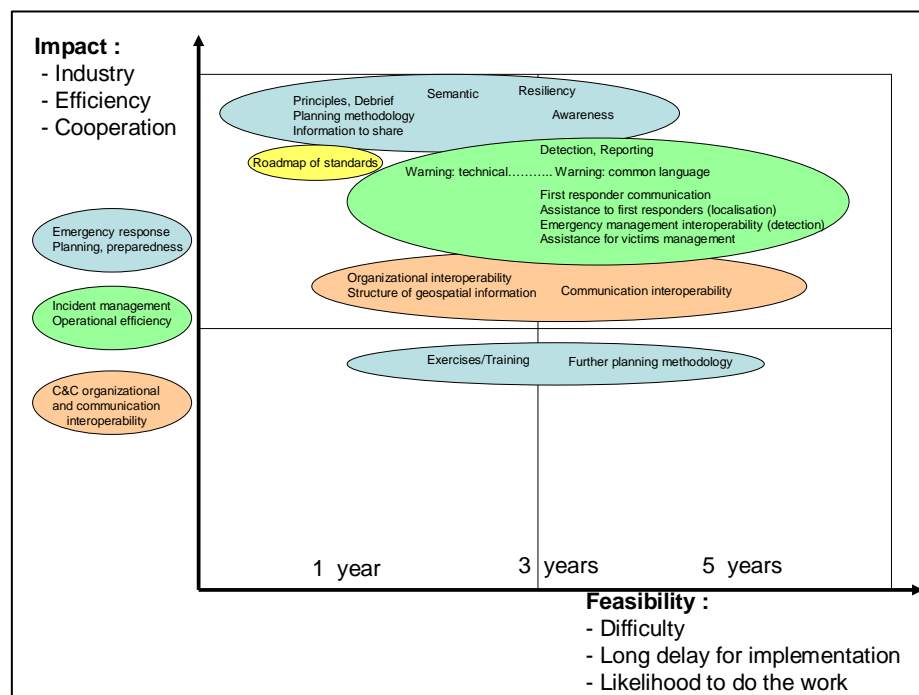


Figure 9: High level standardisation roadmap for crisis management (Source: Final report Phase 2)

¹⁰⁵ Final Report Phase 2 “Proposed standardisation work programmes and roadmaps” (2013)

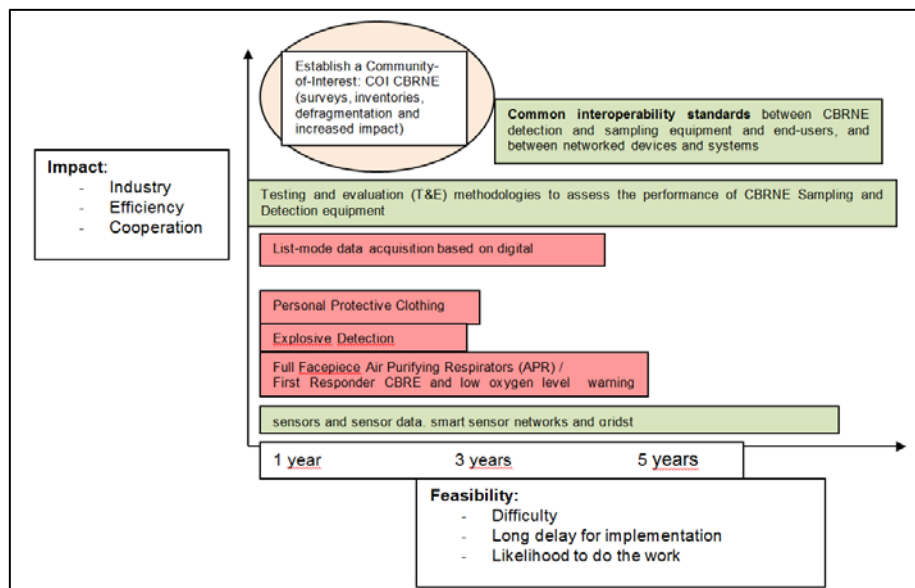


Figure 10: High level standardisation roadmap for CBRNE (Source: Final report Phase 2)

Prior to finalisation of the Phase 1 report, the draft report has been circulated to the involved stakeholders for comments. The final report was first approved by the members of CEN/TC 391, after which it was presented to CCMC for submission to the CEN and CENELEC BTs for approval. Upon approval of the BTs, the report was submitted to the EC.

The expected duration of Phase 2 according to the mandate was six months; in practice it was eight months. The Phase 2 final report was submitted to the EC in July 2013, 11 months after the start of Phase 2.

3.2.2 Review of the implementation phases

General approach

The general approach taken by the EC to structure the work on M/487 in these two phases, with having the first phase as a „preparatory phase“ focusing on fact finding and preparing the ground for executing Phase 2 was appropriate as regards the lacking overview of the EC of the standardisation landscape in security, as mentioned before – and it was in line with the approach taken in M/415. This approach was in particular appropriate at the time of issuing M/487, as funding of dedicated standardisation activities e.g. via FP7 was not possible. This has changed in H2020, where now standardisation projects can be funded like research and innovation activities, as it is the case with the ResiStand project – which now would allow to e.g. include the need for such a broad analysis of the security standardisation landscape in a dedicated H2020 CSA, which could do such a preparatory study as it was done in Phase 1 on M/487 – possibly within a broader time frame and a substantial funding, allowing for the active involvement of a larger group of security stakeholders including end users, industry and academia as project partners, providing funds for stakeholder workshops, etc. In turn, the work to be done in executing the Programming Mandate would be released from such preparatory work and could concentrate on the identification and assessment of the concrete standardisation needs and opportunities.

Phase 1 – Preparatory study

The approach taken within Phase 1 is seen appropriate as well, and was sufficiently implemented by the organisation executing M/487, given the time and budget constraints. With regard to the requested time period of 8 months for Phase 1, not much more could have been asked for. While in particular the European and international standardisation landscaping, as well as the survey of relevant FP7 projects provided comprehensive overviews, the result of the national surveys and the security stakeholder mapping could have been more extensive – if project time and any budget would have allowed for it (it has to be noted, though, that all 18

member countries of CEN/TC 391 had been involved in the national standardisation survey, of which 11 responded in the one way or the other, but only 5 countries provided lists of their national standards in the area of security). Also, the active involvement of the "security community" in Phase 1 through e.g. participatory measures such as dedicated „landscaping workshops“ per security sector would have contributed to the level of detail and comprehensiveness of the stakeholder mapping, but certainly would have exceeded the time frame provided by the mandate – and the financial resources of NEN which could have been dedicated to this activity.

The main result of Phase 1, the prioritization of those security sectors "in particular need" of accelerated standardisation proved useful, as it enabled the EC to select therefrom three areas to be addressed in detail in Phase 2 – and by reflecting these three areas in official Communications, namely COM(2012) 417 Security Industrial Policy and Action Plan. Furthermore, the approach taken by the mandate and the results of Phase 1 achieved were welcomed by security stakeholders, e.g. EOS, the European Organisation for Security.

The stakeholder mapping in Phase 1, however, was too generic to be of much use for Phase 2, so it had to be detailed for the selected sectors in Phase 2.

Phase 2 – Standardisation programmes and roadmaps

The general approach for Phase 2, at least from the point of view of the EC, was appropriate as well, as it specified the expected results, but left open the way how to achieve these results in the given time and budget frame by the contractor, allowing for its necessary flexibility. And, most importantly, in contrast to Phase 1, Phase 2 was financed by the EC. In this sense, the concrete approach for Phase 2 executed by the contractor was appropriate too, as it pursued to allow for widest possible and active involvement of the sector specific security communities in Phase 2, by:

- subcontracting well experienced stakeholder experts (one for each security domain) after an EU-wide Call for the Expression of Interest, tasked to lead the analysis in their respective domain,
- complementing the general stakeholder landscape from Phase 1 for the selected security sectors, and setting up stakeholder lists with contact details,
- collecting standardisation needs and opportunities ("gap analysis") through a survey involving the identified stakeholders (including the members of CEN/TC 391),
- complementing the findings from the survey through interviews of key stakeholders by the three experts, and
- executing one stakeholder workshop per sector to review the results from the survey, and to prioritise them with regard to the standardisation programmes to be proposed.

While this work approach proved effective, it turned out that the quality and the usefulness of the outcomes of the stakeholder workshops as the corner stone of the analyses in Phase 2 was depending on the composition of the stakeholders participating and their expertise, and the way how the workshops were structured and moderated. As this fact accounts for all workshops in general, it was not specific to M/487 Phase 2, and as far as known the contractor and the subcontracted experts had made any effort to allow for widest participation of stakeholders in the workshops. However, namely the security sector of "CBRNE" turned out to be too complex and too diverse to be addressed in one workshop sufficiently in all its specifics with a limited number of participants, and probably would have required sub-sector specific workshops – which in turn would have exceeded the duration and the budget size of Phase 2.

The interaction between the EC, the ESOs and the contractor for both phases seemed to be sufficient for the purpose of the mandate, by applying various means of interaction (meetings of the Coordination Group M/487, frequent emails, phone calls and/or web meetings between the actors). As far as the EC was concerned, the (unforeseen) fluctuation of the policy officers responsible for M/487, resulting in total in four different staff members in charge (working on the mandate as such, supervising Phase 1 and Phase 2, and the follow-up until now) certainly proved as a challenge to all parties involved to ensure the consistency of the work on M/487, and the rationale behind it. From the side of standardisation, the process is rather complicated due to the involvement of multiple organisations, representing various groups:

- CCMC represented the ESOs, but as CCMC includes only CEN and CENELEC, ETSI needed to be separately involved. As ETSI is differently structured, this was challenging.

- NEN was involved as they hold the secretariat of CEN/TC 391. CEN/TC 391 was asked by the BTs to coordinate the work associated with the mandate and the JWG to handle the response. Despite the interest of CEN/TC 391 and JWG members in the work, members were limited in available time to spend on the mandate work. This resulted in most work being done by NEN. This was especially challenging in Phase 1 as there was no funding available. However, as the work is on behalf CEN/TC 391, the work still needs to be approved by CEN/TC 391 and BTs.

These constructions resulted in many layers of discussions and need for agreements and approvals before being able to submit the reports to the EC. If the results of Phase 2 have been useful and provided added value to the EU, actually is an open question. Technically, the request as set out by the mandate and the work as proposed by the contractor had been completely fulfilled. The final report of Phase 2 contains detailed and prioritised lists of identified standardisation needs per security sector, including a high-level description of a possible standardisation work programme. Practically, however, the “concrete standardisation mandates” to be issued to the ESOs by the EC, based on the results of Phase 2 as announced in the mandate, have not materialized themselves until today. The question to be raised also in the further context of this project is, why this process started stuttering, and if this was an implication of failed objectives of M/487, or of other framework conditions. Initial discussions with persons involved in M/487 indicate that certain preconditions are not existent yet (legal acts), which would have allowed for the issuing of standardisation mandates in the three security sectors, and the lack of appropriate budget to finance the execution of these standardisation mandates. The border security sector is a specific one, as it is the only one of the three with an EU Agency in place (FRONTEX), which is organising the cross-border collaboration of the EU Member States, including the addressing of harmonisation needs e.g. for Automated Border Control Systems, and which seemed to have sorted out with the EC in the aftermath of M/487 to take over the lead on the standardisation activities in this sector, by focusing on work within ISO.

3.3 Follow-up of mandate M/487

3.3.1 Description of the follow-up

Completion of work

The report on Phase 2 of M/487 was submitted to the EC in July 2013. In the years following, follow-up actions were taken by both the EC and the standardisation organisations.

The priority areas CBRNE and Crisis management are in the scope of CEN/TC 391 ‘Societal and citizen security’. CEN/TC 391 established a working group in CBRNE already in 2009, but at the time of the execution of M/487 it did not have a working group focussing on Crisis Management. At its meeting in October 2013, CEN/TC 391 therefore decided to establish a working group titled WG3 ‘Crisis Management and Civil Protection’. The first task of this working group was to review the outcomes of M/487 and to identify key topics and possible new standardisation projects. To enable the discussion on the M/487 crisis management results to be wider than just within WG3, a conference was organised during which possibilities and needs regarding standards development in the field of crisis management were discussed with a wide range of European stakeholders¹⁰⁶.

Based on the outcomes of M/487 further mandates from the EC were expected, requesting for the development of specific standards in the priority areas. In its letter to CEN/CENELEC regarding ‘Future standardisation activities on security area on the basis of M/487’ dated 10 October 2014¹⁰⁷, DG ENTR invited CEN/CENELEC to implement the findings from M/487 and to initiate the development of standards for nine specific items, deriving from the M/487 report. Furthermore, DG ENTR stated in its letter that “a new mandate is not appropriate because there is no specific Union legislation to which the requested standards should be linked”.

¹⁰⁶ <http://www.cencenelec.eu/news/events/pages/ev-2014-08.aspx>

¹⁰⁷ Letter from DG ENTR to Mr Vetsuypens from CEN/CENELEC, 10 October 2014, ref. ENTR G4/BC/ap entr.g.4(2014)3608928

The Commission suggested developing the following nine standards:

1. EN (European Standard) serving as glossary for Crisis Management,
2. EN serving as Guidance for emergency response planning,
3. EN on debrief principles for Pan-European exercises and cross-border crises,
4. semantic and organisational EN,
5. EN of map objects and geospatial based information,
6. EN serving as glossary for the CBRNE area,
7. EN serving for full face piece air purifying respirators,
8. EN streamlining education, training and exercise in the CBRNE area, and
9. EN on CBRNE in healthcare facilities.

In its response letter to DG ENTR, CEN/CENELEC stated that for seven items (all except no. 5 and 7) within the scope of CEN/TC 391, this TC would initiate work on these items, providing that the proposals would be accepted by the TC members and at least 5 members would be willing to work on the development. The letter did not specify a timeframe for these developments¹⁰⁸. For the remaining two items (items 5 and 7 in the list above), no technical body would be in the position to develop standards. The item on full face piece air purifying respirators should be discussed by the Unit responsible for the Personal Protective Equipment Directive and the CEN PPE Forum, since this standard might be developed under the ongoing PPE standardisation mandate. The developments and status of the items mentioned above are described below.

CBRNE

During the execution of M/487, CEN/TC 391 was already developing a Technical Specification (CEN/TS) on CBRNE Education, training and exercise. The number of CBRNE experts in CEN/TC 391 decreased after the finalization of the M/487 report, which led to this specific development to be put on hold end of 2014, due to a lack of experts able and willing to work on this subject. To be able to continue or restart the development of this standard, as well as a CBRNE Glossary standard and the standards on CBRNE in healthcare facilities, CEN/TC391 needed to attract more CBRNE experts. One option to ensure the commitment of a selected (group of) expert(s), is to fund the development of a standard under the Framework Partnership Agreement between the EC and EFTA and CEN/CENELEC. The Technical Board of CEN (CEN/BT) decides on the spending of the FPA funds available for subjects in the scope of the CEN/TCs. CEN/BT decided to fund only the development of the EN on CBRNE in healthcare facilities, which was initiated in 2015. Even though no funding was made available, CEN/TC 391 did start the development of the CBRNE Glossary in 2015 as well. Due to the lack of CBRNE experts committed to develop standards, the TC decided to focus on the glossary first and possibly initiate the Education, training and exercise standard at a later stage.

Crisis management

The four items related to crisis management were discussed within CEN/TC391, as well as during the conference mentioned above. During the discussions within CEN/TC 391, and specifically its WG3 Crisis Management, it became clear that the stakeholders active in standardisation, did not automatically see the need for the same standards as the stakeholders consulted during M/487. Furthermore, CEN/TC391 experienced discussions about the understanding of the term crisis management. Depending on language and country of origin, experts understand crisis management to be either the management of major events threatening the community (e.g. disasters) or a business discipline comparable to risk management, business continuity management, etc.

In 2014 and 2015, two standardisation activities related to crisis management were initiated:

- Guidance for Crisis Management, and
- Key Performance Indicators for Crisis Management.

¹⁰⁸ Letter CEN/CENELEC to DG ENTR, dated 2 March 2015, reference DSM196, subject 'M/487 – Reply to your letter on future standardisation activities in the area of Security'

So far, the experts active in CEN/TC 391 have not initiated the development of specific standards for the items requested by the EC, although the Guidance for Crisis Management will touch upon emergency response planning, terminology and semantics as well. For the crisis management related items, no requests for funding have been submitted to CEN/BT.

Full face piece air purifying respirators

Regarding the specific item of full face piece air purifying respirators, CCMC stated in its letter to DG HOME that 'a discussion with the unit responsible for the Personal Protective Equipment Directive (89/686/EC) and the CEN PPE Forum would be necessary'. So far, this discussion has not taken place and no action has been taken regarding European standardisation for full face piece air purifying respirators. It should be noted that in the meantime, within ISO standards for respirators are being developed. These standardisation activities also include standards for CBRN-related respirators. These standards might be adopted as European standards in the future.

Map objects and geospatial based information

So far, no action has been taken to develop standards for map objects and geospatial based information within CEN/CENELEC.

Indirect effects

Even though the aim of M/487 was to establish roadmaps for standardisation activities, the mandate did have an additional effect on standardisation. Stakeholders involved in standardisation, and specifically in CEN/TC391, realised during and after the execution of the mandate that multiple TCs working on standardisation related subjects within CEN do not always cooperate and communicate in the most efficient way. To explore if the very diverse security-related standardisation activities can be coordinated more efficiently and effectively, a workshop will be organised end of 2016, in which representatives of CEN/TCs, national standardisation committees, and liaised organisations and research projects, will discuss possibilities to coordinate their activities in the future.

The M/487 reports were the first to give a clear overview of the European security standardisation landscape. Even though the primary aim was to serve as roadmaps for standardisation activities, the reports are often used for other means. Many research projects use the reports as a source for their own standardisation-related research, e.g. for a more specific area within security standardisation. Furthermore, the overviews of standardisation committees and possibilities given in the reports are often used by stakeholders to connect with the right committee to get involved in standardisation.

One of the conclusions of M/487 was that the European security market is highly fragmented and that standardisation organisations, end-users, industry and research could all benefit from closer cooperation. The "EU Community of Users on Safe, Secure and Resilient Societies"¹⁰⁹, in which mainly research projects connect, communicate, cooperate and look for synergies has been inviting standardisation organisation to participate in its events, in order to narrow the gap between research and standardisation.

3.3.2 Review of the follow-up of M/487

As it was requested by the mandate, in Phase 1 the contractor identified in total six security sectors as "priority areas" for security standardisation (border security, aviation security, CBRNE, crisis management and civil protection, personal data protection, and "general coordination of security standardisation"). The Final Report of Phase 1 was submitted to the EC on 09 May 2012, and only two months later, on 26 July 2012, the EC published COM(2012)417 "Security Industrial Policy and Action Plan", which in its Action 1 referenced the objectives and the work of M/487, and selected three out of the six proposed security sectors (border security, CBRNE and crisis management/civil protection) by specifying them in this Action 1. Clearly, a faster and more consistent response of the EC to the results of Phase 1 would have been impossible.

¹⁰⁹ <https://www.securityresearch-cou.eu/>

As far as known, the response of the EC to the results of Phase 2 was also without any delay. The Final Report of Phase 2 was accepted almost immediately, and – after the change of the desk officer in charge of M/487 at the EC – the responsible unit at DG ENTR entered into bilateral discussions with the relevant policy DGs for these three areas (namely DG HOME with FRONTEX for border security and CBRNE, and DG ECHO for crisis management/civil protection) to jointly assess the findings of and proposed priority standardisation actions in the Final Report Phase 2. And here it seems to have turned out that the limited level of detail provided by the analyses undertaken in Phase 2 challenged these discussions, as necessary in-depth information was lacking. This challenge, and the change of the staff in charge, likely had an impact on the further uptake of the results of Phase 2.

According to its own planning, the EC intended to issue concrete standardisation mandates per selected priority security sector to the ESOs already in the second half of 2013. Until now, this has not happened, for the reasons mentioned: missing legal basis, lacking of budget, difficulties encountered because of the unplanned change in the staff involved, and the lacking of the necessary detail of individual standardisation needs identified in Phase 2. In addition it turned out that even a widest possible involvement of stakeholders in the Phase 2 workshops did not ensure that identified standardisation needs which had been identified there would have been welcomed and shared by other stakeholders active in TCs of CEN/CENELEC, even if from the same nation and/or organisation involved. So, a consistent presence of actively involved experts from security stakeholders throughout all stages of standardisation, from the preparatory work done in Programming Mandates until the concrete standardisation work in TCs and CWGs seems essential for the success of such top-down standardisation actions of the EC.

4 Conclusions and recommendations

Although some PIs have been identified on national and international level, most programming initiatives can be found on European level, the so-called mandates. Conclusions for all levels are provided below, while the conclusions for European programming initiatives are provided in more detail and including recommendations.

4.1 *Conclusions for national programming initiatives*

On national level, one German programming initiative on electric mobility was identified and analysed. Here the national government initiated a platform for an efficient information exchange of relevant stakeholders and to develop a work programme for electric mobility in general and related standardisation activities as one aspect in particular. Additionally a project for setting up a standardisation framework is funded by the government. Its core tasks is the integration of research results, the monitoring of existing standards and ongoing standardisation activities on national, European and international level, the provision of a stakeholder contact point, the support of roadmapping activities for standardisation and the coordination of international cooperation in standardisation.

Based on the above, the creation of such a platform is recommended. This recommendation is combined and included in Recommendation 8.

4.2 *Conclusions for international programming initiatives*

On international level, very limited information regarding standardisation-related programming initiatives could be identified. In the UN framework, programming initiatives as the 'Sendai Framework for Risk Reduction' was conducted. Standardisation is considered as an important and effective measure to pursue the objectives but specific standardisation programming initiatives could not be identified. However, there is an endeavour by the UN to contribute to standardisation work on the one hand and by standardisation organisations to consider the work done by the UN on the other hand.

There are no recommendations based on the analysed international PIs.

4.3 *Conclusions for military programming initiatives*

Next to the civil PIs, also the military PIs have been analysed. The defence sector uses either civil, dual-use or specific military standards. Efforts are being made to exploit civil-military synergies in the area of research and development. The EC has, in cooperation with EDA, recommended the development of so-called hybrid standards. Cooperation between civil and military organisations for standard development may experience issues due to security and classification.

There are no recommendations based on the analysed military PIs.

4.4 *Conclusions and recommendations for European programming initiatives*

The initiation of standardisation in a “top-down approach” by the EC is a mean to accelerate European standardisation in those areas, where there is a concrete need identified from the point of view of EU policies and legislation. Mandates are a tool for the EC to request the ESOs to develop standardisation work programmes in specific areas and/or develop specific standards.

Based on relevancy for the area of security and disaster resilience, mandates were selected and analysed. Table 2 provides an overview of these mandates, including some background, result of work and the lessons learned.

Table 2: Investigated European programming initiatives in the field of security and disaster resilience

Programming Initiative	Year	Background	Standardisation request(s)	Results of work conducted	Lessons learned
Mandate M/419 – Standardisation mandate addressed to CEN for the development of a series of standards on supply chain security	2007	<ul style="list-style-type: none"> - 2004: Initiation of Secure Operator legislation initiative - 2005: Installation of expert group for supply chain security at CEN - 2010: Withdrawal of Secure Operator legislation initiative 	<ul style="list-style-type: none"> - set up of a detailed standardisation work programme - adoption of new/updated standards within 3 years 	<ul style="list-style-type: none"> - establishment of CEN/TC 379 in 2008 (closed down again in 2014) - two standards developed 	<ul style="list-style-type: none"> - set up of expert group to identify actions facilitated work - study about need for standards conducted by neutral standardisation external organisation - need for standards was not seen by stakeholders as anticipated by EC which could point at a lack of early stakeholder involvement - ISO activities do not seem to have been fairly considered in mandate execution
M/487 Programming mandate addressed to CEN, CENELEC and ETSI to establish security standards	2011	<ul style="list-style-type: none"> - 2008: Council Directive 2008/114/EC on the identification and designation of European critical infrastructures - 2008: EC Communication “Towards an increased contribution from standardisation to innovation in Europe”, COM (2008) 133 - 2009: ESRIF Final Report - 2009: EC Communication COM (2009) 691 responding to ESRIF - 2009: EC-commissioned „Study on Competitiveness of the EU Security Industry“ - 2009: The Stockholm Programme of the European Council 	<ul style="list-style-type: none"> - first to conduct a security standardisation landscaping, including recommendations for areas in need of standardisation - second to conduct an in-depth analysis of the areas selected by the EC, and to propose standardisation programmes with roadmaps 	<ul style="list-style-type: none"> - Final Report Phase 1 M/487: security standardisation landscaping, proposal of six security sectors for priority standardisation - Final Report Phase 2 M/487: proposal of high-level standardisation programmes with roadmaps and prioritized standardization topics, for three selected areas (border security, crisis management, CBRNE) 	<ul style="list-style-type: none"> - sustained presence of the same personnel (staff and experts) involved throughout all stages required - selection of the “right experts” from all stakeholders, in particular end users is crucial - evolution of framework conditions need to be monitored (budgets, time frames, etc.)
Mandate M/509 – Programming mandate to CEN, CENELEC and ETSI on	2012	<ul style="list-style-type: none"> - 2007 : Lead market initiative with PPE as one focus market 	<ul style="list-style-type: none"> - set up of standardisation work 	<ul style="list-style-type: none"> - proposals for standardisation activities 	<ul style="list-style-type: none"> - economic and political background gives good support

Programming Initiative	Year	Background	Standardisation request(s)	Results of work conducted	Lessons learned
protective textiles and personal protective clothing and equipment		<ul style="list-style-type: none"> - 2007: Installation of task force for PPE by EC - 2008: Action plan for protective textiles - research projects results under FP7 	<ul style="list-style-type: none"> programme - develop new and revise existing standards 	<ul style="list-style-type: none"> - installation of horizontal CEN/CLC TC for PPE - PPE Sector Forum strategy 	<ul style="list-style-type: none"> - results of research projects as one starting point - strong consideration of end-user needs gives more balanced perspective - horizontal TC as central contact point for TCs and to ISO - involvement of many stakeholders in study about needs facilitates later engagement - no time frame means less pressure
Mandate M/512- Standardisation mandate to CEN, CENELEC and ETSI for reconfigurable radio systems (SDR)	2011	<ul style="list-style-type: none"> - 2011 The initiator for the mandate was the EU and EDA drafted the mandate in co-operation with ESSOR nations and Germany - 2013 The EC requested ETSI to execute the mandate, and to develop harmonised standards, and the request was formally accepted by ETSI in May 2013 	<ul style="list-style-type: none"> -work program to identify items to standardise - a detailed plan for the objectives were requested and made -ETSI invited stakeholders to technical groups 	<ul style="list-style-type: none"> - civil standardisation activities performed by ETSI - in the civil sector technical reports have been published by ETSI 	<ul style="list-style-type: none"> - development of hybrid standards can benefit both civil and military community - a clear timeframe for the work was worked out by EDA - no information about military standards in the mandate execution
Mandate M/530 – Standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management	2015	<ul style="list-style-type: none"> - 1995: right to privacy with respect to the processing of personal data (Data Protection Directive 95/46/EC) - 2011: Establishment of Cyber Security Coordination Group (CSCG) consisting of ESOs for advising on cyber security - 2013: Cybersecurity Strategy of the European Union (JOIN/2013/0001) - White Paper of the CSCG 'Recommendations for a Strategy on European Cyber Security Standardisation' 	<ul style="list-style-type: none"> - to develop European standards for privacy and personal data protection management - related standardisation deliverables for giving practical guidance 	<ul style="list-style-type: none"> - two Technical Committees working on this mandate - first standards initiated/developed 	<ul style="list-style-type: none"> - several communications between ESOs and EC fosters the mandate development - recommendations by the ESOs have been taking into account (are part of the mandate) - a clear timeframe supports the mandated work

The analysis has shown that this top-down approach, if it should become successful and sustainable over the years to be executed, requires particular attention by all stakeholders involved to a number of critical issues and dependencies, i.e. framework conditions, execution of the work, stakeholder involvement and follow-up.

Framework conditions — A European mandate can consist of one of the following elements, or a combination of these: (1) a preparatory study, landscaping the standardisation field in a specific area; (2) development of standardisation work programmes and roadmaps, to understand what the specific needs are in that area; (3) development of specific standards, based on the previously proposed standardisation work programmes and roadmaps. If no preparatory study was done previously, a mandate would request this first before developing a standardisation work programme and roadmaps (e.g. M/487). If a preparatory study is available, a mandate can request a work programme followed by the development of standards (e.g. M/419) or only the development of standards can be requested (e.g. M/530).

The timeframe and funding are different for each of the mandates and depend on the wishes of the requesting authority. Sufficient time and funding to execute the mandate work, but also to follow up on the top-down standardisation actions and recommendations, is essential for the success of such work. In the case of M/487, this was the first horizontal study in the field of security standardization. Due to time and budget constraints, not more could have been asked for than what was conducted, while the results (including more stakeholder involvement) could have benefited from more time and resources.

Recommendation 1: Monitoring of framework conditions (directed to EC)

Framework conditions and their evolution over time have to be considered in detail to the extent possible already at the planning stage of future Programming Initiatives, and closely monitored during their execution, to minimize unwanted effects of unexpected developments. This includes subjects such as the existence of a legal basis requiring standardisation, the support by stakeholders from industry, user-communities etc., sufficient EC budget appropriately prioritised to allow for the funding of top-down standardisation actions, challenges posed by unplanned but inevitable changes in the core staff involved, etc.

Recommendation 2: Setting a time frame (directed to EC)

Setting a time frame for the expected work to be done under the programming initiative, including for the expected delivery of the developed standards, can lead to a more focussed execution.

Execution of the work — The mandates are addressed to the ESOs, to involve all European standardisation bodies in the work. The structure of the ESOs makes it challenging to involve all three entities. To keep it practical, one of the entities acts as the contact point and is responsible to involve the others. The result is that one entity is often more involved than the others. This is also reflected in the technical committees that are involved; if CEN is for example the main contact point, then the involvement of CEN/TCs is usually no problem, but the involvement of the other committees from CENELEC and ETSI is more difficult. Formal commitment is given by all ESOs, but in practice it is often one ESO or TC that is dedicated to the work.

As the ESOs themselves do not execute the work, often the secretariat of the related TC is asked to execute the mandate work. One is very depended on a dedicated chair and secretary to execute the work and to involve all TC members as well as other relevant parties. With all these layers (EC, ESOs, TC, WG, secretariat), the process to accept a mandate work and approval of the reports as a result of the work takes much time.

The analysed mandates were all executed according to the description of the mandate, however some mandated required more time than initially anticipated.

Recommendation 3: Simplifying processes (directed to ESOs)

The mandate work would benefit from more simplified processes at the ESOs, as acceptance of the mandate work and approval of reports involves many layers which is time consuming and often not calculated in the time available to execute the work.

Stakeholder involvement — While the ESOs execute the work, the content of the work is provided by the experts in the field. Involving the ‘right’ stakeholders at the ‘right time’ for the ‘right level of involvement’ is challenging; the TC members represent experts from various European countries that are active in a specific area of standardisation. These experts represent only a part of the stakeholder community; sometimes specific groups of stakeholders are missing, such as end-users. Also, the requirements for joining standardisation work for each country is different and may provide reasons for some experts not to participate to standardisation while being an important stakeholder for the mandate work. This is the reason why in the execution of the mandate work, a wider stakeholder involvement is included. With topics in the area of security/disaster resilience, another challenge arises: these horizontal subjects are more difficult to cover, have an even wider range of stakeholders (that are possibly only partially interested in the work), so ensuring ‘all’ relevant stakeholders to be involved is challenging. One way of addressing such horizontal topics is to divide the topics into sub-areas and to involve experts for each of the sub-areas (e.g. in M/487 three experts were responsible for each of the priority areas and respective workshops were executed, in M/509 four task groups were created with each a task group leader), allowing for more stakeholders groups to be addressed. However, despite or even because of the broad involvement of stakeholders, specific standardisation needs that resulted from the work were not always shared later on by the experts involved in standardisation (e.g. M/419 and M/487).

Involving stakeholders even before the drafting of the mandate or after the finishing of work showed to be very valuable as well. One good practice is M/509 where an expert group was formed by the EC to discuss the needs before drafting the mandate. Another example is the “EU Community of Users on Safe, Secure and Resilient Societies”, meetings organised regularly by DG HOME to encourage closer cooperation and synergy between standardisation organisations, end-users, industry and research.

A strong involvement of user-communities in the study conducted under M/509 led to an added perspective besides the vision of the product-oriented stakeholder structure of the standardisation framework in the area.

Recommendation 4: Ensuring consistent presence of stakeholders (directed to ESOs)

A consistent presence of actively involved stakeholders throughout all stages, from the preparatory work before drafting the mandates until the concrete standardisation work in TCs positively influences the engagement of those throughout the entire process. Preferably the stakeholders are the same throughout the work and will also be the ones developing the standards. Furthermore, it is essential that members of the TCs are committed throughout the work, as well as to take up the standardisation activities deriving from it.

Recommendation 5: Including a broad range of perspectives (directed to ESOs)

Include a broad range of stakeholder perspectives, especially the often underrepresented user-perspective to assure a balanced and widely accepted work programme.

Recommendation 6: Working in sub groups (directed to ESOs)

Horizontal subjects with multiple areas of expertise are complex and difficult to approach. During the mandate work, dividing such a topic into sub groups may be helpful, allowing stakeholders to easier identify their area of interest and to encourage a more focused participation.

Recommendation 7: Installing a horizontal platform (directed to ESOs, EC)

Install a strategic, horizontal platform (such as the EU Community of Users or the national platform on electric mobility) which functions as a meeting point for standardisation organisations, end-users, industry and research related to the topic. It can work as a data recorder, processor and provider in both directions, thus ensuring the required consistency of the work to be done in all phases of standardisation.

One should note that such groups or platforms will need support in terms of funding and resources if the activity should be sustainable, ideally initiated and/or backed by the EC.

Follow-up — In general the follow-up is limited after the execution of the mandate work; often there is a gap between the end of the mandate work and the uptake of the follow-up actions and recommendations due to several reasons. On the one hand, funding is not always available, resulting in a lack of time and resources from experts and standards bodies to take up the standardisation actions or follow up the recommendations. On the other hand, recommendations and actions concerning multiple areas of expertise and being relatively new to standardise, are found to be difficult to initiate. There are already a lot of existing TCs, but these are mainly product oriented. New TCs or groups need to be formed, which takes much time. Also, recommendations that are more user-oriented are challenging, as users are in general not (enough) involved in the standardization process.

A top-down approach does not necessarily ensure that the standardization needs are worked out and/or that stakeholders stay involved.

Recommendation 8: Ensure funding (directed to EC)

To narrow the gap between the end of the mandate work and the uptake of the follow-up actions and recommendations, the organisations addressed to take up the actions and recommendations will need to be supported with the appropriate means in order for them to make time and resources available. These organisations may include the standards bodies, the involved secretariat, the involved stakeholders, and so on.

Recommendation 9: Preparing the uptake of the vision (directed to ESOs, EC)

Recommendations and actions concerning multiple areas of expertise which are relatively new to standardise, are found to be difficult to initiate and will be time-intensive. A horizontal, strategic group already installed during the execution of the programming initiative can ensure the uptake of the vision in the follow up by focussing on a holistic perspective.

Recommendation 10: Strengthen end-user involvement (directed to EC, ESOs)

Possibly comparable to their evolved participation in EU research projects, end-users (and in particular practitioners) might need to experience first that they are needed stakeholders in standardisation, before becoming an active contributor to the standardisation community. EC and ESOs should consider means how to better and specifically involve end-users in standardisation work, e.g. through dedicated standardisation projects in H2020.

Annex 1 Assessment sheet for identified PIs

Assessment Sheet for identified Programming Initiatives

1 Preparation of the programming initiative

1.1 Motivation for PI

- What was the motive to initiate the PI?
- Who is the initiator ¹of the PI?
- Who was involved in the initiation of the PI?
- Has there been a predecessor for the PI?
- What are the high level objectives of the PI?
- What is the expected impact of the PI?

1.2 Design of the PI

- What was the goal of the PI?
- Who was involved in the design of the PI?
- How was the process of the design of the PI?
- Who was responsible for the execution of the PI?
- Who executed the PI?
- Have the Standard Developing Organizations (SDO) been consulted?
- Has there been a request to investigate the need of standards?
- Has there been a specific request to develop standards?
- Has there been a process established on how the PI is to be implemented?
 - Roles
 - Responsibilities
 - Processes
- What was the time schedule for the PI?

1.3 Review of the preparation phase of PI

- Examples of assessment aspects to be addressed:
 - Appropriateness of the approach taken (Programming Initiative) by initiator to achieve the requested objectives
 - Sufficiency of the interaction between the initiator and the ESOs/SDOs in the design process
 - Effectiveness of the execution of the design process by the initiator, the ESOs/SDOs
 - *Other aspects?*

2 Implementation of the programming initiative

2.1 Organization of the work

¹ Initiator is the organization which requested (and likely also developed) the PI.

- How has the coordination group been established, who was in it and what was its role?
- (Optional) What was the structure for the execution of the project?
- What was the assignment of the experts? How were they selected?
- Which methodology was used?
- How was involvement of stakeholders ensured?

2.2 Results of the work

- What were the results (not content, but form)?
- What was the input of the stakeholders?
- (Optional) How did the time schedule influence the results?
- (Optional) How the process was until the report was submitted to the initiator?

2.3 Review of the execution phases of the PI

- Content: see above, to be critically reviewed
- Examples of assessment aspects to be addressed:
 - Appropriateness of the stakeholder involvement
 - Usefulness and added value of the results of the PI
 - Appropriateness of the approach taken (Programming Initiative) by initiator to achieve the requested objectives
 - Sufficiency of the interaction between the initiator and the ESOs/SDOs/executing organization in the executing phase
 - Effectiveness of the execution of the design process by the initiator, the ESOs/SDOs
 - Other aspects?
 - Has the PI been conducted as envisaged?

3 Follow-up of the programming initiative

3.1 Implementation of the PI work results

- Is an efficient and adequate co-operation mechanisms with appropriate technical experts established?
- Has a close liaison with other international programs covering similar topics been established?

3.2 Continuation of PI related tasks after expiration of PI

- Which initiatives have been initiated on the basis of the PI?
- Are these initiatives conducted?
- Do the initiatives involve development of standards by the participating SDO?

3.3 Review of the follow-up of the PI

Can we add concluding remarks about the follow which I think is described in the previous section?

- Content: see above, to be critically reviewed
- Examples of assessment aspects to be addressed:

Annex 2 BT N8625, including the draft resolution for CEN and CENELEC BT



BT N 8625
(Draft Resolution BT C47/2011)
Issue date : 2011-04-14
Target Date : 2011-05-25

BT - TECHNICAL BOARD**1 TO DECIDE**

2 SUBJECT : Mandate M/487 to establish Security Standards

3 BACKGROUND

See Annex 1.

A corresponding proposal is submitted to the CENELEC Technical Board.

4 DRAFT RESOLUTION

BT,

- noting,
 - that EC/EFTA mandate M/487 for requesting a study to analyse the current standardisation 'landscape' in the field of security standards and the development of a proposed work programme. (Annex 1 to BT N 8625) has been sent to CEN, CENELEC and ETSI;
 - that work requested in mandate M/487 in the field of security represents a first step in this very large sector;
 - that EC/EFTA expects to issue future mandates to request the implementation of specific standardisation work programmes based on the outcome of mandate M/487;
 - that, as security is a global field, the analysis requested and subsequent proposed work programmes should take into account existing national, European and International Standards;
 - that the work is relevant to all three ESO;
 - the mandate Work plan in M/487 is in 2 phases:
 - Phase 1: ESO to provide within 8 months the result of a preparatory study and a list of sectors for priority treatment;

- Phase 2: based on EC reaction to the output of Phase 1, ESO to provide proposed standardisation work programmes and roadmaps related to the agreed sectors within 6 months of the acceptance of the report (Phase 1);
- that the EC wishes to have the initial findings at the earliest opportunity and therefore it is anticipated that the work under Phase 1 should itself be carried out in 2 stages:
 - Phase 1-stage 1: provide an overview of the current 'landscape', who is doing what, which areas might be highlighted for priority treatment, followed by an informal check by the EC;
 - Phase 1-stage 2: work on a selected, small(er) number of specific subjects for more in-depth study work.
- decides,
 - to accept mandate M/487
 - that CEN/TC 391 'Societal and citizen security' coordinates the work associated with the Mandate;
 - to ask CEN/TC 391 to establish a specific Working Group to handle the response to Phase 1 of the mandate and develop the Phase 1 report as outlined above and include representatives from:
 - CEN, CENELEC and ETSI;
 - CEN, CENELEC and ETSI technical bodies and other 'technical' groups active in the security field;
 - the bodies and organizations identified in mandate M/487 as being relevant to this work;
 - the interested European Commission services;
 - to establish an informal coordination group (consisting of, but not limited to, the chairman and secretary of CEN/TC 391, the ETSI Security Coordinator and representatives of the ETSI secretariat, CEN, CENELEC and CCMC) which will provide the CEN/TC 391/WG 'M/487 with additional support, information and any guidance it might require in order to provide the Phase 1 outputs in line with the European Commission wishes. In addition, it will keep the Technical Boards informed of progress of the work and if needed be in a position to initiate contact with the wide range of interested bodies, groups and organisations relevant to this work;
 - that Phase 2, which will include the identifying selected sectors for standardisation with appropriate and realistic roadmaps, will be prepared by the corresponding technical bodies of CEN, CENELEC and ETSI, and coordinated by the informal coordination group;
 - to ask CENELEC/BT to concur.

This resolution is applicable as from: 2011-05-25

5 RESP : A Ganesh



CEN Reference: [Annex 1 to BT N 8625](#)

CENELEC Reference: [Annex 1 to BT139/DG8413/DV](#)

Mandate M/487

EC/EFTA have issued to mandate M/487 (see Annex 2 to BT N8625) to the ESO requesting a study to analyse the current standardisation 'landscape' in the field of security standards and the development of a proposed work programme.

EC/EFTA expects to issue future mandates to request the implementation of specific standardisation work programmes based on the outcome of mandate M/487.

As security is a global field, the analysis requested and subsequent proposed work programmes should take into account existing national, European and International Standards.

The mandate is horizontal, potentially covering all subjects relating to civil security and should be executed in close cooperation with the widest possible range of interested groups.

The expectations from this first, horizontal mandate in the large area of security are that the response from the ESO to mandate M/487 will initially consist of:

- an overview of the current status of standardisation,
- identification of the priority subject areas for standards development
- proposals for the range of standards that will be required to fulfil those needs.

In effect, this ESO response will represent the first step to potentially much greater future standards development activity across a wide range of security-related topics.

The mandate Work plan in M/487 is in 2 phases:

- **Phase 1:** ESO to provide within 8 months the result of a preparatory study and a list of sectors for priority treatment.
- **Phase 2:** based on EC reaction to the output of Phase 1, ESO to provide proposed standardisation work programmes and roadmaps related to the agreed sectors within 6 months of the acceptance of the report (Phase 1).

NB. As output of Phase 1, the EC is expecting a single, combined report from the ESO.

Further discussions with the EC confirm that the latter's wish to have the initial findings at the earliest opportunity and therefore it is anticipated that the work under Phase 1 should itself be carried out in 2 stages:



- **Phase 1-stage 1:** provide an overview of the current 'landscape', who is doing what, which areas might be highlighted for priority treatment, followed by an informal check by the EC;
- **Phase 1-stage 2:** work on a selected, small(er) number of specific subjects for more in-depth study work.

Proposed working arrangements – Phase 1- stage 1

In order to provide a single, coordinated report, it is proposed that CEN/TC 391 *Societal and citizen security* would take the overall lead. CEN/TC 391 has a horizontal remit and could provide the necessary focal point for this work. CEN/TC 391 would establish a dedicated Mandate M/487 Working Group to prepare the Phase 1 report, which would include:

- CEN, CENELEC and ETSI representatives
- Representatives of CEN, CENELEC and ETSI technical bodies and other 'technical' groups active in the security field
- Representatives of the bodies identified in mandate M/487 as being relevant to this work
- Representatives of the interested European Commission services.

The Working Group would ensure that the other relevant stakeholder organisations mentioned in the mandate including national agencies, European Technology Platforms and ISO, IEC and ITU-T standardisation groups.

A small informal coordination group (consisting of, but not limited to, the chairman and secretary of CEN/TC 391, the ETSI Security Coordinator and representatives of the ETSI secretariat, CEN, CENELEC and CCMC) will provide the CEN/TC 391/WG 'M'487 with additional support, information and any guidance it might require. In addition, it will keep the Technical Boards informed of progress of the work and if needed be in a position to initiate contact with the wide range of interested bodies, groups and organisations relevant to this work.

The report resulting from Phase 1-stage 1 will be agreed in the CEN/TC 391/WG 'M'487 and provided to the Technical Boards before being submitted to the Commission.

Proposed working arrangements – Phase 1- stage 2

CEN/TC 391 WG 'M/487' will continue to be the coordinating focal point for the work to develop the report, with the in-depth study work being carried out by CEN/TC 391 and other CEN, CENELEC and ETSI technical bodies.

The output of Phase 1-stage 2 will be submitted to the CEN and CENELEC BTs and the ETSI Board for approval and will include proposals for the organization of the work in Phase 2 which will include the identifying selected sectors for standardisation with appropriate and realistic roadmaps.



The following is proposed to the CEN and CENELEC Technical Boards:

- to accept mandate M/487;
- that CEN/TC 391 'Societal and citizen security' coordinates the work associated with the Mandate;
- that CEN/TC 391 establishes a specific Working Group to handle the response to Phase 1 of the mandate and develop the Phase 1 report as outlined above and include representatives from:
 - CEN, CENELEC and ETSI;
 - CEN, CENELEC and ETSI technical bodies and other 'technical' groups active in the security field;
 - the bodies and organizations identified in mandate M/487 as being relevant to this work;
 - the interested European Commission services;
- to establish an informal coordination group (consisting of, but not limited to, the chairman and secretary of CEN/TC 391, the ETSI Security Coordinator and representatives of the ETSI secretariat, CEN, CENELEC and CCMC) which will provide the CEN/TC 391/WG 'M'487 with additional support, information and any guidance it might require in order to provide the Phase 1 outputs in line with the European Commission wishes. In addition, it will keep the Technical Boards informed of progress of the work and if needed be in a position to initiate contact with the wide range of interested bodies, groups and organisations relevant to this work;
- that Phase 2, which will include the identifying selected sectors for standardisation with appropriate and realistic roadmaps, will be prepared by the corresponding technical bodies of CEN, CENELEC and ETSI, and coordinated by the informal coordination group.