EUROPEAN COMMISSION

SEVENTH FRAMEWORK PROGRAMME

THEME Monitoring and tracking of shipping containers
SECURITY

FP7-SEC-2010-3.2-1
GA No. 261795

Cassandra

Deliverable No. D6.3
Deliverable Title Final Protocol
Dissemination level PU/Public
Written By Jan Malenstein (KLPD), Willem Schewe (KLPD), Gerwin Zomer (TNO), Bram Klievink (TUD), Michiel Nijdam (EUR), Wim Visscher (DCA)
Checked by Michiel Nijdam / EUR 31/5/2014
Approved by Heather Griffioen / TNO 31/5/2014
Issue date 31.05.2014
**Summary**

The Cassandra project addressed procedures and methods (protocols) for government supervision of international trade lanes. Specifically, it looked at the impact of the Cassandra innovations on the procedures and methods to assess risks (risk assessment protocols). This covers the way in which the businesses of a specific trade lane interact with government inspection authorities.

More specifically, it was assessed how the Cassandra RBA will enable government organisations to assess the risks of the supply chain better. The Cassandra business RBA, combined with a *data pipeline* for data capture and exchange, enables government to piggyback on data from better sources and on business controls.

To do this steps needs to be taken to move from Trusted Traders to Trusted Trade Lanes, for this the four elements from the AEO framework can be translated to trade lanes. A key topic that needs to be addressed is what comprises sufficient or good level of control over the supply chain. Also, developing strategies for dealing with residual risk is necessary.

The main focus of the Cassandra project was on the ‘good-guy’ perspective, trusted traders that want to optimize their business in cooperation with government agencies. The next step is to also include the ‘bad-guy’ perspective that is more suitable for police related tasks. Severe and organised crime is currently not included in the chain control framework.

The Cassandra EU risk management can be linked to the approach of the EU policy cycle on organised crime. Nine priorities have been defined in the EMPACT framework (European Multi-disciplinary Platform Against Crime Threat). These priorities are:

1. Criminal networks related to illegal immigration.
2. Human trafficking, sexual and labour abuse.
5. Cybercrime, including high-tech crime, child porno and credit card fraud.
6. Organised crime against assets (burglaries, holdups and vehicle/cargo crime.
7. Illegal trade of weapons.

Each of these SOCTA threats can be linked, to a certain extent, to the Cassandra data pipeline. It has to be analysed if Cassandra Supply Chain data can support the police perspective and if it can be linked to the Cassandra dashboard for authorities. It is estimated that there is potential for that with a system based European Risk based Approach protocol that would be satisfactory for the Police, including the following:

- Use data pipeline for backtracking and reconstructing supply chain
- Use data pipeline for typical risk based approach not covered by customs risk engines
- Motivate trusted traders to act as gate keepers and whistle blowers

Moreover, there is Potential of major joint control operations using data in the Cassandra pipeline.
Recommendations

There is a need for a more concerted effort to broaden the scope for policy support for a European Risk based Approach across other policy areas for risk management purposes on transport. Where Cassandra addresses the international trade lanes over sea the other areas of transport: road – water – rail within the EU should be covered as well. This can’t be captured by regulation alone; all parties involved in the supply chain need to express the will to comply with Supply Chain Security in a public – private interaction on a national or EU level.

Not enough risk-related information is made available under current operational methodologies and structures. Since the exchange of information between customs at first point of entry and other relevant Member States, public agencies and other stakeholders is not working properly, information relevant to risk assessment at EU level is being overlooked. The same applies to crime intelligence and mutual analysis results. This operational coordination and exchange of information should be improved on national levels and the EU level.

An AEO application covers a division of a legal entity applying but the AEO-certificate should cover all the activities of the legal entity involved in the international trade supply chain and the criteria will be applied across all those activities.

The development of trusted trade lanes is the next step to also develop further interaction protocols between business and public authorities. The DASC methodology provides an important instrument for businesses to assess their level of control over the trade lane. Furthermore, it offers a good starting point to get into a discussion with supervision agencies and can help them to understand the ‘business’ of the specific trade lane.
## Index

1. **Introduction** .............................................................................................................. 5

2. **Trusted trade lanes, chain control and chain based supervision** .......................... 7
   2.1 Business rationale to manage supply chain risks .................................................. 7
   2.2 Business-government interaction models ............................................................. 8
   2.3 First steps to Operationalize a chain control supervision framework .................. 10

3. **Synergies and complementarities RBA for customs control and combatting serious organized crime** ......................................................................................... 13
   3.1 Common starting point but different paradigms ...................................................... 13
   3.2 SOCTA threads and EMPACT priorities ............................................................... 13
   3.3 Examples of complementary approach to Police ..................................................... 17
   3.4 Potential of major joint control operations .......................................................... 18

4. **Conclusions and recommendations** ...................................................................... 20
   4.1 The Cassandra data pipeline ................................................................................. 21
   4.2 Policy areas and covenants ................................................................................. 21
   4.3 Operational coordination and exchange of information .......................................... 22
   4.4 Vulnerability and reliability of stakeholders ......................................................... 22
1 Introduction

Government agencies – e.g. customs, port authorities, and tax administration – fulfil important tasks in international supply chains. Amongst the many tasks, we expect that such ‘supervision authorities’ keep dangerous goods outside the borders, monitor that business are compliant with existing laws and collect taxes accordingly. An important assumption in the project is that government inspection authorities can assess the risks associated with specific trade lanes. Based on this assessment, government agencies such as customs, the police and food and product safety authorities determine the control mechanisms (e.g. physical inspection of a container) they apply to the trade lane.

As a consequence of this approach, system based control instruments can complement an effective control mix, resulting in considerably lower trade transaction costs and control burden experienced by traders. Such control instruments are part of a System-Based Approach (SBA) to supervision of supply chains. In Cassandra, the SBA entails the possibility for government (inspection) authorities to assess the supply chain risks from their regulatory and inspection perspectives, and assess whether businesses are sufficiently in control of their trade lanes. Currently, the key element of the EU’s supervision instruments is the AEO certificate, at the level of individual operators. As part of an SBA, the mix of control mechanisms that is used in government enforcement can be differentiated between trusted traders (e.g. AEOs, of which the controls have been assessed get primarily post clearance audits and conformity checks) and unknown traders (control mechanisms employed are primarily based on physical control and verification of declarations).

This deliverable builds on various previous reports in the project, and is a direct successor to deliverable D2.3 (‘Business-Government Risk Assessment Protocols’). In that deliverable, we expanded the supervision concept from trusted traders to the level of trade lanes, which requires an assessment of the extent in which businesses are in control of risks in their supply chains. In D2.3, the concept of a trusted trade lane is introduced and discussed. Furthermore, based on four workshops, an agenda for explicating the trusted trade lane view on top of the existing trusted trader view (i.e. AEO) was proposed. Especially, more work was needed on the requirements on the specific risks that need to be addressed at a supply chain level, the controls that businesses can put in place, and the specific data elements that need to be acquired in a timelier manner and of a better quality. Given the complexities and specificities of each trade lane, it is not currently feasible to describe these requirements in generic terms, but the process of finding and utilising them is similar for various trade lanes.

In this document, we pick up where D2.3 ended. We have taken the vision on supervision and enforcement, and can look back at how the project has contributed to enriching our understanding of this vision, as well as on how to make it tangible and applicable. This report summarizes our current and evolved understanding of the interactions between businesses and government, in the context of the Cassandra concepts RBA and data pipeline. The material in this document is based on the actual demonstrations in the Living Labs, further research, evaluations, and interaction workshops. Many of the underlying details are covered in empirical project reports (notably the Living Lab deliverables).

Looking back at the project, we also acknowledge that much of Cassandra’s supervision vision starts from a good guy perspective. This is part of the logic of the project, as innovations in supervision as
well as investing in data pipelines suits compliant and pro-active companies best. However, when looking at all risks and threats affiliated with international trade, the Cassandra innovations can only address a part of those. Misuse of trade lanes and other illicit activities in the international flow of goods are ill-covered by Cassandra (vulnerabilities that follow from the technical artefacts of the project are covered, for example in the data security framework (D3.3)). Therefore, in this report, we pay specific attention to a bad guy perspective and reflect on how the project and the main innovations therein are related to that. This is primarily evident by contrasting the customs view on how Cassandra can and should work with the view of police (one of the consortium partners). Also, the chain control framework and the enforcement vision of customs do not address the threats that police is working on, as laid down in the EU Serious and Organised Crime Threat Assessment (SOCTA). In contrasting these perspectives, some interesting findings can be made, for example on the role of AEO’s, the gatekeeper function of traders, inter-agency collaboration, and the risks of misuse of trusted trade lanes.

This report is structured as follows. In the next chapter, we discuss the findings related to customs and other inspection agencies and reflect on how the project has contributed to further specifying the trusted trade lane concept and the instruments needed for operationalizing that. In the third chapter, we discuss the findings of confronting these developments with the bad guy perspective. Finally, in the fourth chapter, we draw conclusions and make suggestions for a future agenda.
2 Trusted trade lanes, chain control and chain based supervision

2.1 Business rationale to manage supply chain risks
All economic actors choose and apply strategies to cope with business risks, all in different ways, depending on their role and position in their stakeholder environment. For supply chain risk management, the Risk Based Approach identifies four key ways, the 4-Ts: Terminate or avoid risks, transfer risks, tolerate or accept risks and treat or control risks. The choice for applying this portfolio is driven by economic rationale, risk versus return.

A growing group of economic actors has effective control measures in place to cope effectively with the most pertinent supply chain or business risks as well as the most pertinent risks identified by customs. As a consequence, they hold the Authorised Economic Operator (AEO) certification or plan to achieve this. Here, we assume that the supervisory role of customs is a sufficient guarantee that these economic operators are compliant and sufficiently trustworthy by the way they manage the risks identified in the AEO-guidelines. How the customs control supervision process is being executed is being elaborated in the next section.

CASSANDRA has recognized differences in the way trusted traders cope with business risks, the 4T-portfolio mix. This is mainly driven by commercial interests (risk-return-vulnerability-impact), sometimes explicitly formulated, sometimes more implicit choices. Also the way they apply supply chain risk management differs from (over)structured to unstructured or ad-hoc ways. For managing customs risks, all AEOs have applied a structured way according to the AEO-guidelines.

But the research has shown that managing business and supply chain risks and managing customs risks not always go hand in hand. Transferring and accepting business risks are not always effective ways to cope with customs risks. And in some cases business objectives and customs objectives deviate, which means that corresponding business control measures are not always effective.

A key finding is that having a set of effective business control measures and being able to monitor its effectiveness provides the basis for a trusted trader status – they are in control -, recognised by the AEO certificate.

But there is more. Businesses that are in control manage their business risks in a satisfactory way. But this might still imply there is a residual risk for customs. The RBA-analysis has shown that particularly chain control measures often include both business and customs risks, resulting in small residual risks. Moreover, the evaluation deliverables D5.4 and D5.5 highlight the strong business economic rationale of applying some chain control measures. Accurate and reliable data as basis for both efficient supply chain decisions as well as accurate and complete declarations is such an area. An obvious example elaborated in CASSANDRA is the validated packing list (by a tallyman) that also provides the basis for pre-arrival declarations. Obviously, such chain control mechanisms form one of the ingredients of the concept of trusted trade lanes. The next paragraph describes the business-government interaction models for unknown traders, trusted traders and also for trusted trade lanes.
2.2 Business-government interaction models

To develop an interaction protocol between commercial parties and government organisations it is of importance to identify which part of the chain is trusted to provide reliable data. The basic categorization in three levels of trust is helpful to determine the way to design the interaction.

- **Unknown traders**: intensify supervision on transaction level, including physical inspections to check conformance between physical layer and information layer.
- **Trusted traders (AEO)**: Piggy back on internal control mechanisms according to AEO-self assessment; AEO Audit, monitoring, supervising AEO with help of Desk Audit and Field Audit.
- **Trusted trade lanes (TTL)**: An option is to apply a similar framework as the existing AEO-framework, with guidelines, open norms, self-assessment and interaction process between the trusted actors in the supply chain, exchanging supply chain security information.

![Figure 1: unknown traders, trusted traders and trusted trade lanes (Source: Dutch Customs, 2013), see Deliverable 2.3](image)

An important existing instrument is the AEO certificate. The AEO certification starts with a self-assessment by a company (a principle-based approach). Based on the self-assessment and depending on the way a country has organised it, often customs experts (the auditors) engage in a discussion with the company. The self-assessment covers the risks that the business identifies and the control measures or solutions that they have in place. In the Netherlands, a common practise is to use a scale from 1 to 5 to rank the maturity level of the effectiveness of the control measures.
Based on the combination risk-measures they score themselves (0-5). Documentation of procedures (level 3 score) should be the minimum, but for use in Trusted Trade Lanes, businesses should have monitoring systems in place (score 4).

Cassandra looks beyond the level of individual operations of actors and addresses risks at the level of trade lanes. This also means that business operators need not just assess the risks and control measures they have in their own organisation and at their own premises, but also the risks and (potential) control measures for their end-to-end supply chain. This often needs to be done with respect to the specific type of goods, trade lane and actor constellation. This means that businesses need a supply chain wide assessment of data-sources, processes, risks, mitigation and control measures. This is needed to support a government assessment of the trustworthiness of a trade lane at the trade lane level (instead of individual companies). In deliverable D2.3, we described how this affects the supervision approach that can be employed by customs. In short, it was argued that the AEO certificate is a proof of being a trusted trader, but that trusted trade lanes go beyond that in control over the supply chain. Trusted trade lanes could therefore be considered a special category, potentially eligible for a different mix of supervision instruments applied to them (e.g. emphasis on conformity checks and system audits instead of physical border inspections).

There is some resistance from trade groups and individual organisations for a further level of differentiation. They claim they are already in control – recognised by their AEO-certificate -, the fear is that further differentiation would implicate increasing transaction costs to comply to such an AEO-TTL status. Aiming for broader recognition of a trusted trade lane by other (border) control agencies would certainly help overcoming this resistance factor. Furthermore, in the Living Labs, business rationales were found to exist for improving control at the trade lane level (see Living Lab reports and D5.2).

Now, what distinguishes a trusted trade lane from a trade lane with one or more trusted traders (or even those comprising only trusted actors)? Cassandra did not manage to fully develop a chain-based supervision concept. Still, in the process of developing the Cassandra RBA, the data pipeline architecture and their application in the Living Labs, valuable lessons were learned on why it is difficult to change the existing business-government interactions. Furthermore, we found tools and instruments that can be used in further developing and applying new supervision concepts and altering the business-government interaction protocols. The Dutch practice of scoring levels of control, might be a good instrument for trusted trade lanes as well (in the Netherlands, the Promenade project of customs, TNO and branch organisations of logistics parties and shippers, led to a similar AEO Capability Maturity Model). See the Capability Maturity model in Figure 2.
The next paragraph identifies some of these elements that could be considered as key elements of a trusted trade lane concept.

2.3 First steps to operationalize a chain control supervision framework

The operationalization of the trusted trade lane concept can for a large part build on the elements that are in place for the AEO framework. The four elements in this framework that are also applicable for the trusted trade lane are:

- Guidelines
- Open standards
- Supervision and audit by customs
- Interaction procedure to discuss tailor-made supervision and control interventions by customs

Ingredients for a chain control framework and basis for guidelines may include:

- Chain visibility (e.g. by implementing a global data pipeline)
  - Chain mapping and capturing key events (see DASC-methodology in D4.1 report and separate white paper), 'decomposing' a trade lane in goods/services, actors, processes, IT systems, and data
  - Chain of custody/audit trail: Capture transaction linkages on aggregation/consolidation: order – shipment (expedition), shipment – container (stuffing/consolidation), container - vessel (ocean terminal)
- Ensure high data quality
  - Ability to access data from the source, use where possible non-aggregated data
- Query source systems (or data integrators) using a standardised interface ('piggybacking')
- Ability to know how good/reliable the data are (can be done using the DASC methodology)
- Data triangulation or verification
- Validate data against historic or irregular patterns
- Coach suppliers /upstream partners to provide you with right data in right format
- Restrict ability to change/adjust data
- Built-in-controls at vulnerable moments and hubs along the value chain;
  - Tallyman at container stuffing validating packing list
  - Security levels for access to data
  - Check at reception of the goods: proof of delivery
  - Check at container release from terminal on recurring customs status of consignments
- Chain control & container integrity monitoring system (ensure effective functioning)
  - Monitoring carriage/operation: T&T, exception reporting
  - Monitoring container integrity: CSD, container seal checks, ..
  - Internal and external audits
  - Monitoring customs legislation
- Contractual control and INCOTERMS choice. A contract of carriage between buyer and seller often specifies the distribution of responsibilities and liabilities along the transport chain. By actively steering on applying certain INCOTERMS to purchase or sales contracts, buyers or sellers have the ability to 'internalise' decisions to apply chain control measures. Most extreme options include buying under EXW-conditions or selling under DDP-conditions. Of course, the contractual control applying these INCOTERMS still could mean that processes in the value chain will be outsourced, but now you can apply your own outsource strategy, including partner selection criteria (e.g. AEO-certified).
- Partner selection & screening; distinguish recurring partners and incidental partners, with corresponding procedures and monitoring mechanisms.
  - Incidental transaction based screening: For instance when a customs broker gets a request to submit an import declaration as Direct Representative or Limited Fiscal Representation. The screening procedure could include checking email addresses (e.g. Hotmail addresses), quality and professionalism of the business website, way of communication (e.g. Blackberry use). But it could also imply checking the identity in commercial trustworthiness databases (e.g. Dun & Bradstreet) up to full due diligence investigation.
  - Screening procedure for new network or outsource partner: 2PL, 3PI, 4PL Service providers, agents, brokers.
  - Attention for multi-tier compliance screening, e.g. by checking how your suppliers screen their suppliers, eventually through supplier audits.
  - Check against the use of system-based certification schemes like AEO/CT-PAT, TAPA, ISO, within your partner network
  - Random checks on partner performance
- Facilitate remote scanning, for instance in-house scanning by freight forwarder with interface to customs
- Allow for voluntary information exchange or optional dual filing
  - True consignee / final destination
  - Transparency / openness business information
  - Implementation can range from providing references to additional sources in declaration messages (e.g. ENS) to having data feed from pipeline to customs systems directly

The operationalization of this concept is just at the beginning. Further applied research is necessary; the CORE project will further elaborate the operationalization of a trusted trade lane supervision model. A key topic that needs to be addressed is what comprises sufficient or good level of control over the supply chain. Also, developing strategies for dealing with residual risk (i.e. what is acceptable residual risk for a business may not be acceptable for inspection agencies) is necessary. Cassandra contributed by providing: 1) a business approach to identify and exchange data, 2) a method for business to provide of data beyond legal requirements, and 3) a way for government to extract these data and use it.
3 Synergies and complementarities RBA for customs control and combating serious organized crime

3.1 Common starting point but different paradigms

Serious crime abuses the sophisticated and well developed supply chain infrastructures, including the major hubs and networks for a substantial part of illegitimate trade. Chain visibility and trusted trader programmes help combating the unwanted exposure to organized crime activities. As such, the chain control framework is complementary to support compliant and trusted traders and also combating serious crime. But these two approaches also have different viewpoints requiring different approaches. The two different paradigms include:

- **Good guy perspective: facilitate legitimate traders where possible (AEO and beyond)**
  - The CASSANDRA Global Data Pipeline concept frames in this paradigm
  - Key role for Customs in facilitating this approach by their supervision and enforcement strategies
- **Bad guy perspective: EU Serious Organised Crime Threat Assessment (SOCTA)**
  - Key role for Police in their supervision and enforcement strategies
  - Value of Global Data Pipeline concept is ‘rather limited’, except for some specific areas elaborated in section 3.3.

In order to better understand the bad guy perspective, the next paragraph elaborates on the SOCTA threats.

3.2 SOCTA threads and EMPACT priorities

The EU Serious Organised Crime Threat Assessment is the product of systematic analysis of law enforcement information on criminal activities and groups affecting the EU, and is designed to assist strategic decision makers in the prioritisation of organised crime threats. It has been produced by strategic analysts in Europol’s Analysis and Knowledge Unit (O2) and external partners to produce an assessment of trends and potential future developments in organised crime.

SOCTA2013 has defined 10 priorities, designed to assist strategic decision makers like the European Law Enforcement Working Party (ELEWP), Europol and Frontex in the prioritisation of organised crime threats. In the perspective of Cassandra this may apply to both business- and governmental strategic analysts and decision makers.

EU governments cooperate in an EU policy cycle on organised crime. This cycle will guide operational police cooperation to tackle organised international crime within the EU in a multi-disciplinary framework. The cycle prioritises a number of criminal phenomena based on the SOCTA and negotiations between the member states and has been defined in the COSI (Comité pour la Sécurité Interne) framework in Brussels.

All 9 EMPACT projects have been condensed in MASP’s (Multi Annual Strategic Plans); these MASP’s have been worked out in concrete action plans. Synergy and complementarity with the Cassandra approach for the police has to focus on combating serious organised crime. Key point in combating serious organised crime is the principle “follow the money”. Following documents like cargo manifests etc. has proven to be less efficient and more cumbersome but may be used in conjunction
with the Cassandra dashboard for custom authorities. An important issue to consider is that if it concerns illegal activities, documents probably already may be fraudulent. The integrity of the documents/data in the Cassandra pipeline is assumed to be integer unless it can be proven to be otherwise by Custom authorities. But money and money transfers are real and can be tracked, backtracked and monitored by police more reliable.

A logical thing to do from the police perspective is to link the Cassandra EU risk management to the approach of the EU policy cycle on organised crime. For the period 2014 – 2017 nine priorities have been defined and condensed in 9 projects in the EMPACT framework (European Multi-disciplinary Platform Against Crime Threat); these are:

10. Criminal networks related to illegal immigration.
11. Human trafficking, sexual and labour abuse.
14. Cybercrime, including high-tech crime, child porno and credit card fraud.
15. Organised crime against assets (burglaries, holdups and vehicle/cargo crime.
16. Illegal trade of weapons.
17. Counterfeiting with risks for public health.

**Illegal immigration human trafficking and sexual and labour abuse (SOCTA 1&2)**

Illegal immigration, human trafficking and sexual and labour abuse concern human beings and not commodities and goods. There are simply no cargo manifests or bills of laden on persons, the only documents referring to human beings are passenger- and crewmember lists but these kind of documents do not reveal if there is illegal immigration or some kind of abuse; they indicate a presence at a certain time on a certain moment. Passenger- and crewmember lists are not in the Cassandra pipeline. Data and documents for the police to work with are the lists afore mentioned and personal travel documents like passports. For those personal travel documents a dedicated system is used by border control authorities to check the authenticity and integrity and this can’t be linked to the Cassandra pipeline.

**Drug networks and drug trafficking (SOCTA 3 & 4)**

Drugs are commodities as are the components to manufacture synthetic drugs. As such the latter may be listed under the name of their individual components and may occur on cargo manifests. Police can use this data in an application that generates all possible combination of components in certain transport container that may produce synthetic drugs or explosives! This is tested on a small scale in the Netherlands. Pure drugs like marihuana of cocaine/heroin will in general not appear on cargo manifests unless listed and approved as medicines or for medicinal purposes, this is rather easy to check using the data in Cassandra. Drugs concealed in the flow and transport of goods may be indicated in risk analysis methods used by custom authorities. The origin – destination data in Cassandra can be used by those risk analysis methods.
Cybercrime, including high-tech crime, child porno and credit card fraud (SOCTA 5)

Cybercrime is relevant within Cassandra related to the security framework for the data pipeline, as discussed in WP3. A risk exists that cybercrime methodologies are used as a tool to manipulate the data pipeline, so that criminal organisations can conceal their operations or utilise the data pipeline to facilitate their operations. The other cyber related criminal activities are not within the scope of the Cassandra project.

Organised crime against assets and illegal trade of weapons (SOCTA 6 & 7)

Organised crime against assets consists mainly of stealing goods from ships, vehicles, containers and warehouses. The cargo manifests in Cassandra are very useful to indicate exactly what and how much was stolen. But criminals do not use documents to steal goods or to burglar into a warehouse. Only on the occasion of roadside cargo crime, criminals sometimes use fake documents to divert delivery of goods to a criminal’s address. A truck driver can check by phone at the company when in doubt and company staff can check it using Cassandra data.

When criminals obtain goods from their criminal activities they do not use any documents to do so. But even criminals often have to transport their illicit goods and if these are large quantities it will have to be transported by ship, train or truck and then documents are needed. These documents may be present in the Cassandra pipeline disguised as genuine documents but with proper data analysis tools it may be revealed that something is suspicious with a certain transport.

The same applies to the illegal trade of weapons. Weapons are traded legitimately all over the world by weapon manufacturers to supply armies for instance. Such transports will have all necessary documents present in Cassandra. For illegal weapons trade there are two options: either concealed in regular transports or with fake documents posing a shipment of weapons as legitimate or that the transport contains other goods like scrap for instance.

Counterfeiting and international tax fraud (SOCTA 8 & 9)

Branded products are counterfeit to benefit from success of this branded product (intellectual property fraud). Historically, counterfeit goods tended to be items such as cigarettes and brand name clothing. In recent years, the range of counterfeits has widened to include items such as medicines. Commodity counterfeiting is facilitated by commercial globalisation and the existence of cheap labour.

Counterfeit goods enter the EU via all major seaports before being distributed throughout the EU. The largest volumes pass through Rotterdam, Hamburg and Bremen. China continues to be the main source country for counterfeit goods destined for the EU. Chinese organised crime groups are particularly active in the production, transport and distribution of counterfeit cigarettes, clothes, shoes, toys and pharmaceuticals.

Organised crime groups abuse the sophisticated and well developed supply chain infrastructures, including the major hubs and networks for a substantial part of the SOCTA-related illegitimate trade. Trusted trade lanes, like authorized economic operators, are subject to the risks of misuse because of fewer physical inspections due to their AEO-status. A trusted trade lane benefits from facilitations
with regard to customs controls. Once an organised crime group has infiltrated in a trusted trade lane, there is a lower probability that a container is being scanned by Customs or is subject to physical inspections. However, it is more difficult to abuse a trusted trade lane, because an authorized economic operator takes a many security measures. So this is why an AEO can play a role as a gatekeeper.

9) International tax fraud

VAT fraud is a highly lucrative crime. The economic and social impact of VAT fraud, therefore, is substantial: it distorts the functioning of the single market, accounts for the loss of significant public revenue and affects the financing of the European Community budget. The costs involved in Member States’ efforts in preventing and combating VAT are also significant.

Excise fraud is made possible because of the differences in excise duty between countries. This means that the price of the same product can differ widely in different countries, which gives rise to attractive profit-making opportunities. Examples of such products include cigarettes, alcoholic drinks and mineral oils.

Customs fraud occurs when existing customs regulations are misused, such as the ‘in-transit’ system within countries of the European Union, which provides the possibility not to pay levies when exporting to countries outside of the European Union.

VAT carousel, Customs and excise frauds involve (virtual) goods crossing borders. Goods are transported to other countries via several (apparent) links in order to conceal the true origin and/or the true nature of the goods. Legal entities play an important role because they can set off VAT. Front companies often play a role in smuggling in order to conceal the contraband. When the goods are marketed (paper) companies are used to conceal the true origin of the goods.

Again, organised crime groups abuse the trusted trade lanes, like authorized economic operators. They are subject to the risks of misuse because a trusted trade lane benefits from facilitations with regard to customs controls, like fewer physical and documentary controls.
3.3 Examples of complementary approach to Police

In Cassandra D2.3 a risk based assessment and the business – governmental interaction approach was described, captured graphically in a scheme. This can be linked to the police perspective on combating serious organised crime as follows:

It has to be analysed if Cassandra Supply Chain data can support the police perspective and if it can be linked to the Cassandra dashboard for authorities which at the moment strongly focus on custom user requirements. It is estimated that there is potential for that and if proven so this would fit a methodology for a system based European Risk based Approach protocol that would be satisfactory for the Police approach on serious organised crime and supply chain security.
3.3.1 Use data pipeline for backtracking and reconstructing supply chain
Criminals develop highly complex logistics chains with multiple trans-shipment points and different transport modes to create lack of visibility and ‘smoke screens’ for fiscal fraud. Reconstruction based on the CASSANDRA audit trail can help understand these practices and enhance targeted approaches.

3.3.2 Use data pipeline for typical risk based approach not covered by customs risk engines
Example of synthetic drug production. Inbound of raw materials from different directions and in different shipments, each shipment not subject to high risk profile and import compliant with customs regulations, but pattern of deliveries to a certain location creates enhanced risk. Police could use the data pipeline to build risk engines with algorithms grouping on end location and potentially harmful ingredients or products related to synthetic drug production.

3.3.3 Motivate trusted traders to act as gate keepers and whistle blowers
Complementary to the risk assessment by control agencies and authorities, the compliant trading community has more capabilities to assess certain threats. They could choose to work according to compliant internal procedures and/or not accept dubious orders, but they can also proactively inform control agencies. If the latter leads to intervention by control agencies with considerable negative commercial implications, the incentive to do so is low. The challenge lies in how to identify these trusted traders within the legislative framework.

3.4 Potential of major joint control operations
In The Netherlands it is common practice that integrated controls take place on a regular basis. These integrated controls are always executed in a multi-disciplinary way. Law enforcement agencies co-operate with customs, and several inspections, such as: veterinarian inspections, environmental inspections, etc., etc. These controls are called MACO’s (multi agency control operations).

A huge potential for EU-wide collaboration in major control operations of the different control agencies exist:

- AQUAPOL (EU waterborne police network) has about 15 major yearly European MACO’s in which many countries participate (figures).
- RAILPOL (EU railway police network) organizes several MACO’s on a regular basis and also “24-Blue action days” during which days all trains and train stations are “painted blue by railway police”
- TISPOL (EU traffic police network) organizes more than 15 MACO’s during a year
- FRONTEX (EU agency of border police organizations) has its head quarter in Warsaw Poland and several sub locations in the EU on strategic positions in the Schengen territory. FRONTEX focusses mainly on flows of migrants, facilitation of illegal migration, etc. However FRONTEX also organizes High Impact Operations, which can be compared with the MACO’s of the earlier mentioned networks.
- EUROPOL is leading in the so-called EMPACT-cycle. In other and previous chapters it has been explained, that EUROPOL coordinates the EU efforts in the field of organized crime and the 9 mentioned priorities. EUROPOL works closely together with all member states. In the EUROPOL headquarters in The Hague, all EU member states have their own liaison bureau
and more than often in these liaison bureaus not only police men and women are working there, but also custom officers. This creates good possibilities for a closer co-operation in the fight against organized crime and terrorism. Two of the nine priorities in the EMPACT-cycle are customs related or even their core business. The EMPACT-cycle will lead to many OAP’s (operational action plans) during the period of 2014 – 2017.

- Customs major control operations.
  DG Taxud (Department Taxation and Customs Union) and OLAF (European Anti-Fraud Office): yearly 15 to 20 EU wide control operations in the field of tobacco and cigarette smuggling, drug trafficking and the risk of intellectual property rights violations (Intellectual Property Rights).
  - WCO (World Customs Organization): the WCO and the United Nations Office on Drugs and Crime (UNODC) initiated the Container Control Programme (CCP) for the purpose of enhancing port surveillance in developing countries to minimize the risk of maritime containers being exploited and used for illicit drug trafficking, transnational organized crime and other forms of fraudulent activity.

**Integrated controls and the CASSANSDRA Data Pipeline concept**

Despite the fact that we have not explored ways how the CASSANDRA Data Pipeline could contribute to such integrated controls, we can identify possible ways of application. One example is for instance by linking number plate recognition ANPR to NCTS records (transit movements). An interface with Data Pipeline could identify traders involved in this transaction and cargo details, which might trigger detailed physical control of the cargo. The Coordinated Border Management agenda has not been explored in CASSANDRA, however, the project CORE offers room to further elaborate on these kinds of complementary cases, with the involvement of national customs and WCO, national police and INTERPOL and national food safety control agencies.
4 Conclusions and recommendations

The Cassandra project addressed procedures and methods (protocols) for government supervision of international trade lanes (see Deliverable D2.2 for business RBA and Deliverable D2.3 for government supervision aspect). Specifically, it looked at the impact of the Cassandra innovations on the procedures and methods to assess risks (risk assessment protocols). This covers the way in which the businesses of a specific trade lane interact with government inspection authorities. More specifically, it was assessed how the Cassandra RBA alters these protocols in the sense that a Business RBA at the supply chain level, combined with a higher quality of crucial data elements, will enable government organisations to assess the risks of the supply chain better. The Cassandra data pipeline and the business RBA enable government to piggyback on data from better sources and on business controls; data on the real parties behind the transaction and the movement of goods (buyer and seller or owner), and on the precise goods involved, is essential as is information on the routing of the goods throughout the supply chain (see Deliverable D5.2 for evaluation of the Cassandra outcomes with respect to this).

The project also drafted a Risk Management Protocol, aiming at a new approach to secure international trade through voluntary and economically beneficial contributions and participation by businesses and more timely and accurate data and intelligence provided to government. The Protocol (see also Deliverable D2.3.1) formalises the Piggy Back principle where government draws on data and systems held in the commercial sector used to buy, pay for and ship goods between buyer and seller or consignor and consignee along the length of the international supply chain. It does not depend on administrative rules but on the attitude laid down in agreements. The Risk assessment protocol has considered the opportunity for government agencies to rely on the adequate assessment of regulatory, safety, security, compliance and fiduciary risk by businesses as part of or alongside their normal assessment of commercially based risk.

On the business side, economic operators are crucial to risk management because of the information available to them and the measures they take to secure their supply chain. Existing interaction protocols for AEO’s can be extended to trade lanes when both the organisations and their links can be trusted. It is assumed that the supervisory role of customs will be a sufficient guarantee that these economic operators are compliant and sufficiently trustworthy in the way they manage the risks identified in the AEO-guidelines. To develop an interaction protocol between commercial parties and government organisations it will be of importance to identify which part of the chain can be trusted to provide useable and reliable data. Trusted traders ensure a well-functioning efficient supply chain and manage or mitigate their commercial risks effectively, though the corresponding trade lanes might still be subject to security threads.

A common minimum standard of automated risk analysis for security and safety has not yet been achieved due to variance in the development, capacity and technical capability of national electronic risk analysis systems. As a result common risk criteria cannot be properly monitored and evaluated for effectiveness at EU level; this limits EU capacity to adapt and respond to common risks and hinders innovation in risk management.

A number of conclusions can be drawn from the work undertaken in Cassandra on the issue of policy support for a European Risk based Approach (ERBA).
4.1 The Cassandra data pipeline
The Cassandra business RBA, combined with a data pipeline for data capture and exchange, enables government to piggyback on data from better sources and on business controls. Business that are in control of their supply chains at such level that we can talk of a trusted trade lane, should provide accurate data on the goods and parties involved in those trade lanes. Furthermore, they should have full insight in the operations, controls and data sources in their supply chain, and discuss this with inspection agencies. This helps customs and other inspection agencies to understand the business and to use that understanding in the supervision of trade lanes. Furthermore, source data should be available in the data pipelines and they are opened up to the businesses through a dashboard. On top of the various business dashboards, the Cassandra customs dashboard was designed to support the pre-arrival risk assessment process by enabling customs officers to search the data pipelines for data on shipments, beyond what is available in the summary declarations. This customs dashboard primarily fits the requirements of customs agencies that do not want to ask extra data, but do want to offer business the possibility to voluntarily provide them. The system of summary declarations stays in place, but if the risk targeting system selects a shipment to be further looked at, the customs officer can use the dashboard to see what data from upstream supply chain is available.

This way, the Cassandra data pipeline is a data source for risk assessment by the government, mainly customs, focussing on validation of documents and supply chain when goods are entering the EU. Customs has a risk analysing tool to select controls on those incoming goods to perform its core mission on tax (including smuggling) and possible crimes. An alternative (preferred by another customs partner) is that the data pipelines feed customs systems directly, although the technical implementation thereof poses specific challenges.

Other government agencies like the police concentrate on serious organised crime as one if its main priorities. Where customs use information on goods a priori, police uses information on persons first. Synergy and complementarity with the Cassandra approach for the police has to focus on combating serious organised crime. Key point in combating serious organised crime is a principle called “follow the money”. Following documents like cargo manifests etc. has proven to be less efficient and more cumbersome but may be used in conjunction with the Cassandra dashboard for custom authorities. An important issue to consider is that if it concerns illegal activities, documents already may be (or probably are) fraudulent. The integrity of the documents/data in the Cassandra pipeline is assumed to be integer unless it can be proven to be otherwise. But money and money transfers are real and can be tracked, back-tracked and monitored by police reliably. As such, the Cassandra pipeline may be complementary to but not a substitute for the “Follow the money” principle of the police. It has to be analysed in more detail if Cassandra Supply Chain data can support the police perspective and if it can be linked to the Cassandra dashboard for authorities, which at the moment strongly focus on customs user requirements. It is estimated though that there is potential for that and if proven so this would fit a methodology for a system based European Risk based Approach protocol.

4.2 Policy areas and covenants
Goods do not rest in the ports where they are landed; it is transported by other transport modalities into the inland and hinterland, splitting up a cargo that has arrived by ship into a port into a number of smaller transport entities.
This can’t be captured by regulation alone; all parties involved in the supply chain need to express the will to comply with Supply Chain Security in a public – private interaction on a national or EU level. This can be done by contracts but a better way would be to initiate covenants in which parties commit to cooperate and exchange information mutually. Such a covenant exists in the Netherlands where a second 5 year term covenant has been signed and agreed recently among all the stakeholders in the supply chain: transport union – transport companies – police – insurance – public prosecutor’s office on cargo crime. This would substantiate the Cassandra principle that public agencies can piggy back on business data and vice versa in the EU and could provide the base for a European risk based Approach. Without such basic arrangements the interaction between business and government will remain scattered and ineffective in the area of a common EU Risk based Approach in the supply chain.

4.3 Operational coordination and exchange of information
In principle the focus within Cassandra is on the interaction between business and governmental bodies. Traffic arriving at first points of entry frequently includes cargo bound for other Member States as well as cargo transiting the EU en route to a final destination in third countries. This means that the knowledge and information available at national and local level in the Member State of destination is critical for effective risk analysis and risk mitigation at points of first entry.

In addition, information on parties and their characteristics, including vulnerabilities relating to parts of the supply chain outside the EU, is clearly of common relevance and significance for risk analysis all along the external border. Any significant weakness in information-sharing undermines the effectiveness of risk management at different entry points and for the EU as a whole.

Not enough risk-related information is made available under current operational methodologies and structures. Since the exchange of information between customs at first point of entry and other relevant Member States, public agencies and other stakeholders is not working properly, information relevant to risk assessment at EU level is being overlooked. The same applies to crime intelligence and mutual analysis results. This operational coordination and exchange of information should be improved on national levels and the EU level.

4.4 Vulnerability and reliability of stakeholders
The AEO (Authorised Economic Operator) programme has been firmly established in the EU now. Authorised Economic Operators take significant measures to secure the supply chain and are formally validated by customs authorities. These measures relate to investment in physical security and internal control systems, financial solvency, risk assessment of the business and the reliability of business partners. The AEO’s assimilated to a certain level tasks and roles that originally were performed by customs authorities. It is assumed that the supervisory role of customs will be a sufficient guarantee that these economic operators are compliant and sufficiently trustworthy by the way they manage the risks identified in the AEO-guidelines. AEO is governed by European Community law. The basic law is set out in Council Regulation (EEC) No 2913/92 (the Customs Code).

One might say that AEO’s have taken up the role of being the sentry at the gate; the procedure on how to achieve one of the three AEO levels are documented in detail in the Council regulation but there are some weaknesses. An application covers a division of a legal entity applying for the AEO;
but the AEO-certificate should cover all the activities of the legal entity involved in the international trade supply chain and the criteria will be applied across all those activities.

There is an option that criminals use existing transport streams to sluice in their illicit goods; goods that obviously will not be recorded in the original and correct bill of laden. This stealth option occurs frequently, cocaine hidden in fruit or in engine oil for instance.

The development of trusted trade lanes is the next step to also develop further interaction protocols between business and public authorities. The DASC methodology (see D4.1) provides an important instrument for businesses to assess their level of control over the trade lane. Furthermore, it structures the assessment in such a way (by decomposing the trade lane in goods, actors, processes, systems, and data) that this offers a good starting point to get into a discussion with supervision agencies and can help them to understand the ‘business’ of the specific trade lane. If companies can show and prove to inspection agencies that they are in control and are able to assure quality of data and integrity of the goods flow, inspection agencies can piggyback on the business data (via the pipeline) and business controls, leading to a different supervision regime for those trusted trade lanes. All these elements need to be considered when developing a European risk based Approach in Supply chain security.