



BALTIC SEA INFORMATION MOTORWAYS

WP 2: Port and Supply Chain Security

Lübeck, 28.-29.10.2004

Workpackage 2

Work Package Leader: Germany

Core Partners:

- **Denmark:** Association of Danish Transport Centres
- **Finland:** Finnish Maritime Administration, Port of Turku, Turku Chamber of Commerce
- **Germany:** Port of Lübeck, Technology Centre of Lübeck
- **Latvia:** Ventspils Free Port Authority
- **Poland:** Maritime Institute Gdansk

BaSIM Workpackage 2

Strategic focus:

Improvement of security of transport and logistics by integrated ICT according international regulations and standards.

Planned results:

- Overview on worked out processes according new security regulations in the BSR.
- Best Practice Concept on telematic solutions improving security by telematic integration and support in ports, chains, corridors supported by a demonstrator.

BaSIM Workpackage 2

Result indicators:

Partner's and member's of the Target Groups opinion and further activities according the results of the workpackage and the project as well as the efficiency of the demonstrator. New spatial planning methods on security.

Outputs and their quantifications:

Documented overview of the established processes according security in the selected ports and chains. Best practice concept defining lacks and improvement opportunities exemplified with a demonstrator in a selected port and chain.

BaSIM WP 2, Milestone 1, 09-12/04

Task 1:

Overview on the new processes established in the Baltic Sea Region on basis of the new ISPS-Code, SOLAS convention and IMO regulations. The overview will look at the processes in logistics and transport activities building the basis for a Best Practice Concept and for the demonstrator to be developed.

Task 2:

Identification of ports, supply chains and corridors building the basis for the studies leading to the analysis of lacks and improvement in the sense of the project.

BaSIM WP 2, Milestone 2, 01-06/05

Task 3:

Analysing the selected ports, supply chains and corridors in the sense of the established telematic systems, portals and chains according the correlation to the new processes defined in Task 1.

First preselection of the port and the chain according the technical and security aspects for implementation of the exemplified ICT-based demonstrator.

Presentation of the results and discussion with the partners, users and providers leading to conclusions on the matter and also on further steps.

Task 4:

Preparation and general specification of the Best Practice Concept by defining the lacks in existing solutions and also defining the improvement opportunities and new spatial planning opportunities regarding security. First general specification of the implementation of the demonstrator.

BaSIM WP 2, Milestone 3, 07-12/05

Task 4 (continue):

Definition of the Best Practice Concept looking at the following objectives

- Increase Port Security by means of electronic identification and control
- Increase of Security of goods and their flows in the transport- and logistics-chains by means of electronic identification and control
- Increase the telematic facilities for co-operation and contribution in security of all parties along the chains and corridors
- Increase of data exchange ahead the cargo flows for better forecasting and planning
- Increase Intermodal Tracking & Tracing under the special aspects of exception reporting and reaction

Concept and first implementation activities on the demonstrator in the selected port and chain.

BaSIM WP 2, Milestone 4, 01-06/06

Task 4 (continue):

Definition of the Best Practice Concept showing opportunities and possible telematic supported solutions especially for

- Data exchange and interfaces for security related messages along the transport and supply chains
- Open interfaces for integration of existing systems and platforms
- Intermodal Tracking & Tracing information according international regulations and standards of security
- Functionality for exception reporting and management including interfaces to adequate systems
- Functionality for integration of different identification carriers (barcode, RFID)
- Open platform for customer information of security relevant data

BaSIM WP 2, Milestone 4, 01-06/06

Task 4 (continue):

- High level of data security and data availability. Final implementation of the demonstrator and internal and external testing activities. Final installation. Delivery of the concept to the partners. Presentation and discussion of the results in a workshop. Making the Final Report of the Workpackage 2 and contribution to the Final Report of the BaSIM Project. Dissemination of the results of Workpackage 2 and participation in the Final Conference

Supply Chain Security

The Objectives:

- Increase Port Security by means of electronic identification and control of goods and their carriers in line with international regulations and standards
- Increase of Security of goods and their flows in the transport- and logistics-chains by means of electronic identification and control in line with international regulations and standards
- Increase the telematic facilities for co-operation and contribution in security of all parties along the chains
- Increase of data exchange ahead the cargo flows for better forecasting and planning
- Increase Intermodal Tracking & Tracing under the special aspects of exception reporting and reaction

Supply Chain Security

The Phases:

- Evaluation of the planned and actual processes according security according international regulations and standards
- Evaluation of the demands on telematic view arising from the new processes and from the involved users and their systems
- Concepts on telematic solutions according the results of evaluation and needed functionality
- Development and implementation of a pilot system
- Testing
- Piloting

Supply Chain Security

The Challenges:

- Converting the demands of the international regulations and standards into reasonable processes in daily work
- Final assessment of the demands of the different port situations
- Converting the new processes into telematic solutions
- Integration of different existing systems and interfaces of different levels into a common architecture
- New technical equipment (hardware)
- High level of data security and data availability

Supply Chain Security

Expected Results:

- Transparent end-to-end management of information and goods flows by integrating all players in the chains
- More efficient reaction in cases of exceptions
- Higher security along transport and logistic chains
- Wider information flow
- Increase of quality and cost effectiveness