Secure chain

BACKGROUND STORY

Towards more resilient port logistics

Via the Secure Chain, the business community and authorities are working together to digitally boost the resilience of the port logistics processes. Every initiative that contributes to this is considered. The Secure Chain is a continuous improvement program. Depending on the topic, the partnership will take the lead itself, pro-actively provide parties with input or offer support in the realisation of projects.

Within the Secure Chain, the more secure and reliable release and collection of import containers in the Dutch ports is one of the key focal points. Collaboration is key to this. Data and cargo move from link to link in the logistics chain. Every transition constitutes a potential risk. Through the Secure Chain, only familiar and authorised parties have access to the required information and are able to perform certain actions.

End of the PIN code
The Secure Chain puts an end to the use of PIN codes. In the old approach, the shipping line/ship agent would send the customer a PIN code by e-mail to facilitate the collection of a container. This method was vulnerable to abuse. Frequently, PIN codes would be widely shared within the logistics chain. In principle, anyone who had the PIN code could proceed to the terminal to pick up the container. The Secure Chain puts an end to this. Each link digitally passes on the authorisation to securely collect a container to the next designated party. This creates a closed chain with only familiar, authorised parties that digitally exchange the required data with one another in a secure manner. Furthermore, participants operationally benefit from the smart reuse of data and gain optimal insight into the status and planning of import containers throughout the entire logistics chain.

Implementation via Portbase
The port business community has requested Portbase, in its capacity as the neutral logistics platform of the Dutch ports, to technically realise the safe and reliable release of containers via the Secure Chain. To achieve this, an additional authorisation layer has been created on top of the existing digital services in the Port Community System (PCS). Since many logistics companies already make use of the PCS, the impact of the introduction of the Secure Chain is kept to a minimum. A cost-free basic service has been introduced as an extra option for new parties that need to connect to Portbase for the Secure Chain. As a result, all parties are able to digitally pass on the authorisation to collect a container from one link to the next in a convenient and secure manner. It is crucial that new parties promptly register with Portbase. Connection to the PCS takes time.

The Secure Chain is now practice in the port of Rotterdam for all import containers from Latin America, North America, Africa, Middle East, India and Pakistan. Currently, shipping lines/ship agents are working on connecting customers with cargo from the Far East and Oceania. The end date for this is 3 February 2025. From then on, the Secure Chain will work for import containers from all intercontinental shipping areas. After 3

Secure chain

February 2025, the shipping lines/ship agents also want to route intra-European and feeder cargo through the Secure Chain.

Other program components
One of the other initiatives that the Secure Chain stimulates is the automatic verification of the operating carrier at the gate of a container terminal. By means of this verification, terminals can be certain that the inland operator that comes to collect a container matches the inland operator as specified in the digital pre-notification of the visit via Portbase. This verification is performed by checking the EAN number in the pre-notification against that on the CargoCard of the visiting driver. These EAN numbers are issued by Secure Logistics.

At the ECT Delta terminal, the ECT Euromax terminal (both part of Hutchison Ports ECT Rotterdam), Hutchison Ports Delta II and Rotterdam World Gateway the verification of the operating carrier has already been implemented. APM Terminals Maasvlakte II is preparing. All these terminal operators see the verification of the operating carrier as a logical final step in the process to more securely and reliably release and collect containers via the Secure Chain.

Parties involved and financing
A large number of parties have joined forces for the Secure Chain. Together, they endeavour to boost the digital resilience of port logistics. Combined, the initiating parties represent all the links in the logistics chain: from the shipping line/ship agent, shipper and forwarder to the logistics service provider, inland operator (truck, train, barge) and terminal. The Port of Rotterdam Authority, the Municipality of Rotterdam, Dutch Customs, Seaport Police and various semi-public organisations also support the Secure Chain.

The Secure Chain and its implementation are made possible by, among other parties, the Implementation Agenda for the Port of Rotterdam, National Growth Fund / Digital Infrastructure Logistics and Port of Rotterdam Authority.