BDI: Chain of Trust
Now - challenge  A party with the right information gets access to the chain.

A carrier can pick up a container at a terminal if they have the corresponding PIN code.
Now - challenge  Increasing (drugs) crime in Rotterdam and other Dutch ports. For example, the well-publicised PIN code fraud with containers.

Government needs to look at this, and especially the risk of undermining.

Businesses also recognise need to tackle problem.
How are we resolving this?

From having information to a situation where parties are successively designated as chain partners (release, authorise and nominate).

Secure identities form the basis of the chain of trust in which parties are successively designated – shipping company designates by releasing, forwarder/shipper by authorising and carriers are nominated.

Chain of trust enables an authorised party to perform the activities appropriate to their role, not just on the basis of what information they have.
This ensures that bad actors cannot break into the process based on (the correct) information. They do not gain access to the chain.
The Chain of Trust makes an important contribution to enhancing security around the transportation of containers, but also adds great value as a mechanism for authorised data sharing.