Current process: A cargo handler at Schiphol knows in advance which cargo will arrive when, but not when this will be picked up or by which trucking company.

1. Shipper iPhone4U has ordered a shipment of Apple phones and accessories from China.

2. The cargo handler informs of incoming cargo by means of the flight manifest.

3. Airplane with cargo arrives at Schiphol Airport.

4. The shipment is stored in the handler's depot at the custom's warehouse.
Current process: As soon as the cargo has been cleared by customs, the handler will inform the forwarder (by mail/telephone) that the shipment is ready for pickup.

Notified by the handler, the forwarder creates a transport order for the trucking company and emails any related documents.

The trucking company schedules a pickup, selects a truck and a driver, and registers these in the eRegistration community system.
Current process: On the day of pick-up: the driver collects the shipment at the handler using printed documents.

1. ACN card check and if driver visit has been logged in eRegistration system. It is not checked for which shipment the driver has arrived.

2. Warehouse staff checks the airway bill / documentation and loads the shipment onto the truck. The paper ACN receipt is signed as confirmation of goods received.

3. Trucking company delivers Apple phones & accessories at shipper.

Jansen's name is repeated on different parts of the process flowchart.
Parties in subversie crime know the loopholes in the logistic and administrative processes and possess detailed information of the cargo itself (eg. expensive electronics).

Fake drivers gain access using fake ACN cards and paper copies of airway bills.

**Security issues:**

Prio to pickup, the computer systems only know when a driver is arriving, not for which shipment.

**Security issues:**

With only a paper receipt marked with an unclear signature, it is nearly impossible to determine which driver and company executed the illegal pickup of the shipment.

**Efficiency issue:**

Not knowing the pickup dates/times of various shipments, the warehouse handler can't optimise his workflow (warehouse management problem)
Applying the BDI approach comes with many advantages for this logistical chain with its many contracting parties, the need for real-time coordination and high compliance requirements.

The forwarder can be assured that the trucking company and driver have no knowledge of the shipment’s contents. And that all security checks in the computer systems must be completed before the handler hands the shipment over to the driver. This will improve the quality of his service and minimises payment issues.

Knowing that shipments will be handled securely, with a reduced probability of subversive crime, the shipper can save costs.

The handler knows in advance which driver (from which carrier) will pick up the cargo at what time. This allows him to organize his warehouse more efficiently, saving handling costs.

The handler knows that the cargo will be turned over to the authorized carrier/driver. This reduces the risk of subversive crime and reduces costs for corrective handling at later processing stages.
The core of the BDI approach is to add three additional facilities to the Port Community System of the Schiphol cargo community.

**Authorisation Register**

- Identification
- Authentication
- Authorisation

The first is a standardised ‘zero-trust-API’ including an Authorisation Register for identification, authentication, and authorisation.

Using this API, the forwarder can only select “ACN certified trucking companies and drivers” when scheduling an airwaybill pickup.

If the handler has been authorised to access certain forwarder and trucking company data, he can do so using this API.

To access the relevant data for the pickup, the trucking company must also have be authorised by the forwarder through this API.
Publish/Subscribe The core of the BDI approach is to add three additional facilities to the Port Community System of the Schiphol cargo community.

The second facility is a so-called “event-broker” that uses triggers in the logistical process to proactively distribute events to relevant parties who need this information.

The forwarder will be proactively informed of shipments being ready for pickup.

The handler will be proactively informed of which driver will pick up which shipment and when.

The trucking company will proactively receive the relevant data for pickup – i.e., not including information on shipment contents!

SECURE Parties that have not been authorised for this shipment data, will not have access to these triggers.
The core of the BDI approach is to add three additional facilities to the Port Community System of the Schiphol cargo community.

The third facility is a so-called “Secure eVisit key”, to be validated with an API. A driver will only be able to pickup the shipment if all three elements of this key match in the computer system.
Improved process

Parties will proactively receive the data that are relevant to them and for which they have been authorised.

Parties will be proactively informed using
events that may invoke triggers in their IT systems. The zero-trust API safeguards that only those data will be shared for which each party has been authorised in the Authorisation Register.
Conclusion

A more secure and more efficient logistical process for all parties involved in the multimodal air cargo chain.

A substantially decreased risk of subversive crime.