# Report "Proof Of Concept chain integration TransFollow, carrier and IL&T"

Speaker Title

**TransFollow**

**ahead of the chain**

# Content

# Objective

TransFollow is a platform for exchanging digital waybills and related information. The current market adoption of TransFollow, and with it the digital waybill, has given rise to the demand from enforcement, emergency services and the business community for the necessity and possibilities to make information available to these parties in the context of enforcement and possible calamities.

# Objective

Although there is no legal framework in which the parties are obliged to make the information available in ways other than on paper or on a device (on which the information has been created in the same way and has the same value as paper) there are some practical objections:

- Enforcement is now unable to see a digital waybill in its own environment and check its authenticity. They depend on the cooperation of the driver and the quality and mobility of his device.

- Enforcement is now (with paper) able to see only the relevant document that is maintained. When a device is delivered, more information can be obtained than is strictly necessary (on the digital document and on the device). This is experienced as a threshold.

- In the event of an incident, enforcement and emergency services are now in many cases able to obtain the necessary (paper) documentation independently because it is immediately available in the cabin. With the digital document, they depend on the cooperation of the driver and the quality and mobility of his device.

- Digitalization and standardization has made it possible to obtain information from the Cloud instead of from the cabin, even in the event of a serious emergency. This possibility is not yet being used. Although other initiatives are also emerging here (e. g. eCall and iHeERO), it seems interesting to also investigate the possibilities offered below.

# Objective and scope

TransFollow proposes to realize a Proof of Concept that demonstrates that the above objections can be solved practically. It proposes a mobile portal to which IL&T enforcers can gain controlled access (authentication) after which they can gain controlled access to the relevant consignment note information (authorisation).

It is proposed to allow access to the portal through iSHARE protocols (authentication). As part of the Proof Of Concept, it will be investigated which way of gaining access to the relevant data is possible (authorisation) in which scenarios.

# Interviews

## IL&T - 13 Dec 2017 – Interview with inspector 1/2

IL&T carries out on-road inspections. They are organized by specialized teams. This particular law-inforcer / inspector works on the area of dangerous goods.

The basic process is as follows: on an on-road inspection (generic or at request) the truck is een taken off the road. The driver must then give the CMR for inspection so that the inspector can do his job. The inspector will take it with him to his bus and carry out his checks. The driver may accompany the inspector. The problem with digital freight documents is that the drivers gives more information with his device than just the CMR so the drivers will accompany the inspector more and more which is not preferable. If there has been an inspection, the driver will be provided with an inspection report.

The inspector also simulates what happens with a calamity: are the right equipment and papers available. Also they check for cabotage.

There is no wish from IL&T to see the document on its own device. Authenticity of the document or system is not important for the inspections. As long as documents are available and the information is correct.

# Interviews

## IL&T - 13 Dec 2017 – Interview with inspector 2/2

IL&T foresees problems with accessing digital documents themselves when there will be multiple platforms or when there is a combination of both paper and digital CMR's. If it is not clear where to look in case of an emergency.

In the event of an emergency, the eCMR must be available without the driver's assistance. IL&T would like it to be clear what they should do.

For testing within the POC, IL&T does not see any difference between a calamity and a regular active enforcement check, even though the driver is cooperating, but also wants to test whether he can join the document if the driver is unable to access it.

# Interviews

## Carrier – 12 Dec 2017 - SHEQ manager 1/2

The interviewed carrier now drives with a paper CMR from their customer (the consignor). The consignor creates the document from the place of taking over to its final location. The carrier fetches it from the place of taking over to his own premises with an e-CMR (not TransFollow). There, the trailer is disconnected and checked. Then comes a driver, working at the carrier or a competitor who takes over the cargo. Then they drive with an e-CMR (TransFollow) from their own premises to the final location.

For them it is important that in case of an inspection everything is available and in the event of an incident, everything must be under control.

According to the ADR legislation, there does not have to be any paper CMR in the cabin. In various discussions with IL&T the following was stated:

"According to article 5.4.0.2 from the ADR, Electronic transport documents may be used provided they are "equivalent to a paper copy"". This is explained by IL&T as follows: "It must be clear to the inspector/assistor how the information is accessed without the assistance of the driver. This is done by specifying the steps to be taken in the electronic device, for example, clearly on the device. Whether this complies with 5.4.0.2 is at the discretion of the inspector. Is the information not "easily accessible" or is the battery of the device empty then he should act as if no transport document is present."

# Interviews

## Carrier – 12 Dec 2017 -  SHEQ manager 2/2

For the time being, this carrier only drives in NL with digital waybill because they have the impression that foreign agencies are not yet ready to enforce properly because they are not yet familiar with e-CMR.

Requirements for accessing freight documents:

- The eCMR may be accessible to law enforcers, but certainly not to competitors

- Only the information required for the check may be displayed

- A notification about a law enforcer accessing information is desired. Active authentication to law enforcers is not going to work because then 24*7 monitoring is required

- An overview of which eCMR's have been accessed is desired for checking with the law enforcing reports

- Access based on only the licence plate number in case of an accident is acceptable

- The data from TransFollow may not be used to gauge remotely where someone is driving

# Interviews

## Other important statements

Various interviews have taken place. Most of them gave the same insights as the previous interviews.

Some generic statements are:

- Carriers are reluctant for sharing information with governments for two reasons:
  - Data-security: is their data secure?
  - Add-hoc scanning: is the data used for data-based surveillance
- Carriers are more willing to share information if they are actively informed and real-time notified about queries
- Both carriers and the KLPD prefer to see information on their own device:
  - Carriers for not giving the device containing all kind of other information
  - Law enforcers for not having all kind of devices and not to be accompanied by the driver all the time
- Scanning QR-codes, exchanging pin-codes or active authentication is not preferred for giving access
- Accessing a system like TransFollow is only going to work when there is only one, maximum two eCMR platforms and as long it is clear where information can be found

# Functional requirements POC

The following functional requirements were abstracted out of the various interviews and defined for the POC:

- "As a law enforcer, I want to be able to login to a secure environment to work with TransFollow"

- "As a law enforcer, I want to be able to log in to TF Portal using my own existing account, so I don't have to log in separately at TF"

- "As a law enforcer, I want to be able to search an e-CMR based on its license plate, so I can check the e-CMR"

- "As a law enforcer, I want to view freight documents which are in Transit"

Details (acceptance criteria) are intentionally left out
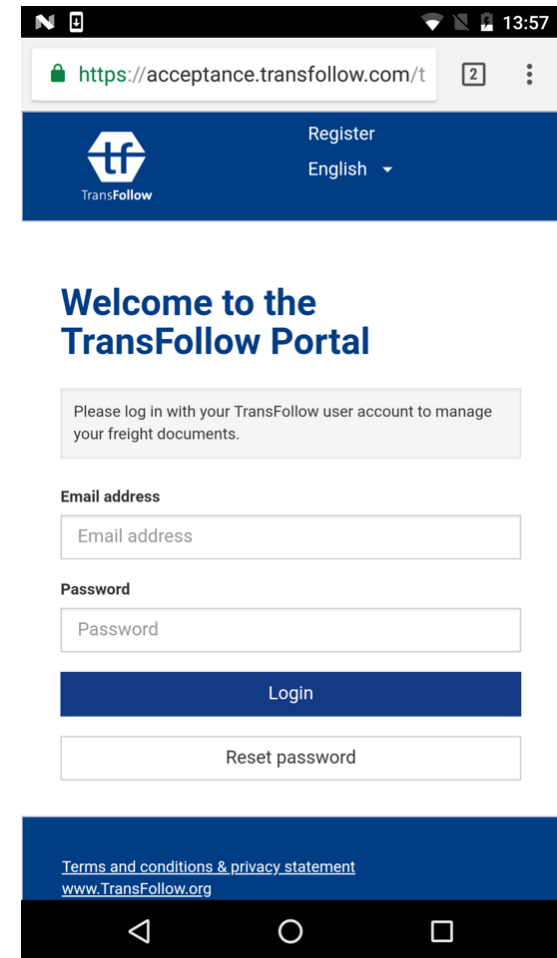
# Portal realisation

## Login

The road-inspector can login to the TransFollow Portal using his credentials. Credentials are person bound and consist of an e-mail address and password.

**Note:** we looked into iShare for logging. Although it has been realised, the limitation of iShare we could not work around is that it does not support generic validated roles therefor we could not distinguish a normal user from a road-inspector using iShare.

# Portal realisation

## Overview of freight documents

When the road-inspector logged in, he enters the freight documents overview screen. Here he or she has the ability to search for a licence plate number.

To be able to search for licence plate we added the infrastructure to add, edit and delete licence plates, per carrier for truck and trailer because this is not part of the (e)CMR.

Licence plates can be entered with or without seperators and are case insensitive but needs to be exact (no wildcards).

**Note:** since the licence plate is not part of the (e)CMR and is mandatory, it is not self-evident that this information is always available and updated correctly. It is therefor advisable to discuss what information is needed for law-enforcers to inspect and regulate this process.

# Portal realisation
## Results

When the road-inspector logged in, he enters the freight documents overview screen. Here he or she has the ability to search for a licence plate number.

The freight documents containing the specific licence plate and for which the status is Issued or "In transit" are shown. Issued freight documents are shown because of the offline signing abilities of TransFollow.

**Note:** during the various interviews, it became clear that there is also a need for checking previous (delivered) freight documents.

# Portal realisation

## View freight document

Once an inspector clicks one of the freight documents to view, the details are opened. He or she has also the possibility to download it as a PDF which is in the same layout as the paper CMR.

**Note:** for the POC, all information is shown to the user. From both parties (carriers and law enforcers) it is a wish to only show relevant information. It needs to be specified what this information is (might differentiate per case).

**Note:** During the field tests, it became clear that viewing the information in a structured and intuitive way is more important that viewing it in the layout of the paper based CMR.

# Additional functional requirements

The following functional requirements were defined but not realized as part of the POC:

- As a carrier, I want to allow be informed (real-time) when a query is done on one of my e-CMR's, so I can check the validity of the query

- As a carrier, I want to know which law enforcement organization has accessed which e-CMR's, so I know which of my trucks have been checked and can match this information with my own reports

Details (acceptance criteria) are intentionally left out

# Field test and first conclusions

Various field tests have been executed and are ongoing.

First results:

- It became clear that there is also a need for checking previous (delivered) freight documents

- Visibility of raw data (screens) is better and preferable above the CMR PDF layout on smaller devices

- After explaining what to do, it is clear how to handle a digital freight document

- To much information is available on the digital freight document and needs to be restricted to what is needed for inspectors

- Some confusion might occur because the online data not necessarily match the real cargo (because of the offline scenario's)
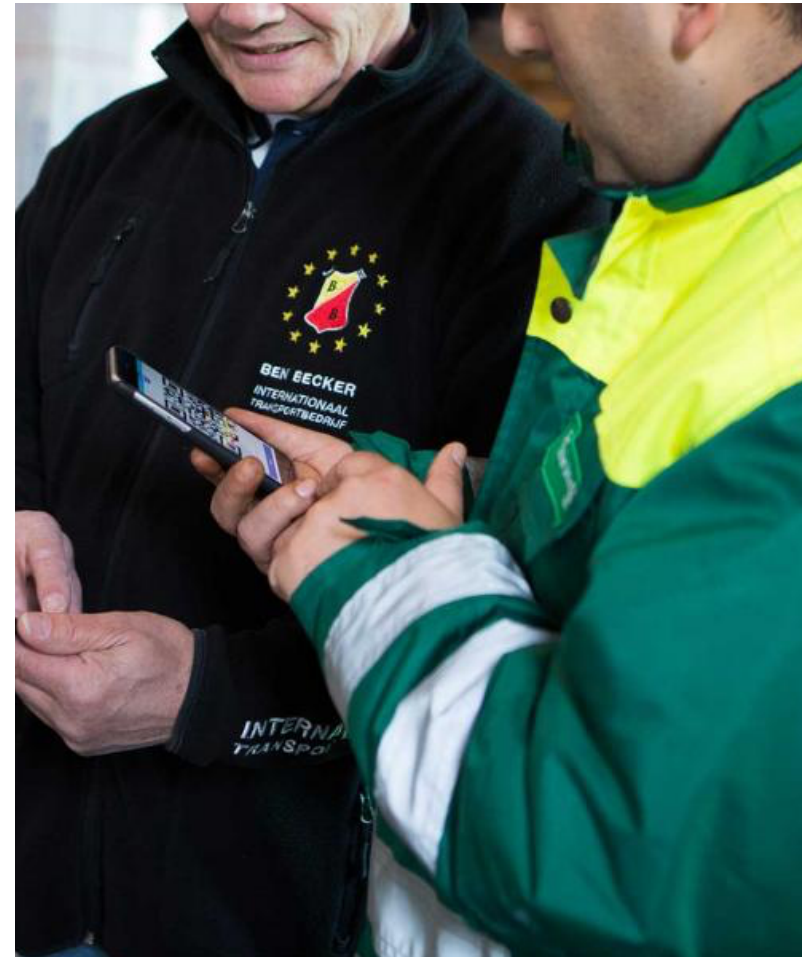
# Recommendations

- There is no infrastructure for giving role–based access to persons to certain centralized databases. iShare should consider adding generic and validated roles so for instance a law-enforcer can access systems as a law-enforcer and have certain access derived from his role instead of having it defined per object

- There is reluctance about sharing information as long as it is not clear what could be done. Clear regulation or awareness is needed

- Both law-enforcers and carriers stated that it is in both interest to have only the necessary information shared. It is recommended to define this data-set with all relevant stakeholders

- A working group to provide a centralized access over the various platforms is needed, preferably on an international level