

JSON Web Signature (JWS) as generic digital proof between organisations



Colophon

JSON Web Signature (JWS) as generic digital proof between organisations

Authors

H. Wagter

S. Schouten

January 2025

© Connekt



Summary

There appears to be an increasing need in business transactions for digital proof for interactions between individual companies, and between companies and supervisory bodies. This involves:

- **Proof of representation (acting on behalf of an organisation)**
- **Transfer of cargo between parties**
 - Collection of a shipment.
 - Unloading of a shipment.
- **Proof of qualifications (when acting on behalf of an organisation)**
- **Proof that rules and laws are being followed**

The people or systems used to carry out the work act on behalf of the companies or supervisory bodies: the organisations are liable here rather than the people, with a few exceptions. It would be useful if there were a way:

- For one party to provide robust (legal and practical) digital proof to the other party rather than having just hardcopy proof.
- To create a work process that suits (varied) practical situations, with changing and sometimes temporary staff who have little IT-related training and limited knowledge of systems and processes.
- To apply the solution broadly at acceptable costs.
- To create a free market for IT service providers who can offer these solutions in a competitive setting.

This document describes a generically applicable method that meets these conditions..¹

After 2010, a new standard² for digital proof has gained popularity: the JSON Web Token or JWT. Currently signed JWTs are used most frequently as proof between IT systems, between servers: they are a tried-and-tested way of sharing permissions and identities of users, are well-known and widely supported.

A signed JWT conforms to the JSON Web Signature (JWS)³ specification). A JWS is the general standard for transferring content with confidence (a document for example), whereas a JWT is specifically aimed at 'claims': the question whether identities can be trusted.

¹ Verifiable Credentials and wallets are a possible alternative that could become widely accepted in the future. A JWT is a compatible format.

² See Annex 2.

³ [RFC 7515 - JSON Web Signature \(JWS\)](#)

The digital proof in a JWS consists of three interlinked parts:

- **Its content (payload)**
 - the claims being made by the sender;
 - possibly with additional data, such as a validity period.
- **Proof that the payload has not been changed since it was sent by the sender**
 - a hash or fingerprint.
- **Proof that the payload plus the proof of 'being unchanged' has truly been sent by the sending party rather than by another party with a false identity**
 - signing (cryptographic operation) using a recognised certificate that belongs to the sender.

High-quality certificates can be used for important data representing a large value. eIDAS certificates ('seals') are one example of this. When these certificates (sealed digital documents) are used, 'signing' will meet the strictest requirements for electronic signatures⁴.

The standard allows JWTs (or JWSs) to be wrapped up in each other. This means that the payload of a JWS may be another JWS, like an envelope inside another envelope. This property is highly practical in logistical applications: it allows the proof that a company is acting on behalf of a client to be delivered all at once. As such there is no formal limit to the number of times 'embedding' can be used, but it always increases the size of the final JWS in kilobytes⁵.

For many applications, convenience is more important than incorporating high levels of security. For these kinds of situations, a version has been developed inspired by the convenience of DigiD and 'Tikkie' payments.

Just like DigiD, users do not require much more than a smartphone, QR code and PIN for this version. The complicated part of the exchange makes use of professional technology between the IT systems of two parties.

The major step forward here is that IT systems exchange 'electronic signatures' on behalf of their companies. They are (digitally) mandated to do so. In this scenario, the people are not the ones 'signing' things. They are interchangeable 'operators' who add a small item of proof to the overall proof that the transfer is proceeding as expected.

⁴ https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.02.01_60/ts_11918201v010201p.pdf

⁵ These large JWSs can no longer be transferred via an HTTP request (header), so they are placed in the body of a request instead.

This overall proof may include things like:

- The time.
- The location.
- The truck's registration number, the carrier's name or the driver's proof of ID.
- The shipment's identification.
- The device used by the warehouse employees, with additional properties such as its IP address, MAC address or other properties.
- The probability that the warehouse employee and the driver are in the same place at the same time and can see each other.
- A picture of the cargo.

This overall proof may be sufficient for the companies involved to have a transfer 'signed' by their IT systems.

The solution is flexible, both in terms of its payload and the option to make changes at the last minute. Its legal strength is high if the implementation is done professionally.

The solution is widely applicable, including for interactions with the government. One example of this is managing privileges for driving empty trucks over a weak bridge.

The Basic Data Infrastructure (BDI) supports this working method in various ways:

- through additional trust in parties ('certification');
- with shared general terms and conditions written specifically for this application;
- with low-barrier hybrid versions, so that parties with limited IT facilities can still be operationally integrated ('Edge Agreements').

Contents

1.	Need for digital proof between organisations	7
2.	Digital proof	8
2.1	Proof of identity and certificates separate	9
2.2	Proof inside proof: useful for outsourcing	9
2.3	Flexible: last-minute changes	9
3.	Application in practice: between companies	11
3.1	Basic DigiDrop	13
3.2	Obstacles	17
	No mobile internet in the warehouse	17
	The warehouse employee cannot scan the QR code	17
	The warehouse employee's device is broken or has no connection	17
	TMSX is temporarily unavailable	17
3.3	A warehouse does not have a DigiDrop provider	17
3.4	Inclusion in general terms and conditions	18
4.	Method for proving training and professional certificates	19
5.	Application in practice for supervisory bodies	20
5.1	Open four corners model for inspections	20
5.2	Providing proof to an inspector	21
5.3	Broader usage: privileges	24
6.	Market forces	26
7.	Support by the Basic Data Infrastructure	27
7.1	Trust in parties	27
7.2	Shared general terms and conditions	27
7.3	Shared semantics	27
7.4	Shared services	27
8.	Hybrid working methods	28
8.1	DigiDrop UltraLite Edge Agreement	28
8.2	DigiDrop Lite Edge Agreement	30
	Annex 1: JWSs and QR codes	31
	Annex 2: Relevant IT standards	32

1 Need for digital proof between organisations

Business transactions (trade and service provision) often include moments when proof needs to be provided between organisations, both between companies and towards supervisory bodies. In current practice, people and hardcopy documents play a key role here.

When focusing on logistics/transport and service provision, the most frequently occurring situations are:

Proof of representation

- Is the person standing here acting on behalf of the original client and for the assignment in question? And can we hold the company where this person works liable for this?

Transfer of cargo between parties

- Collection of a shipment.
- Unloading of a shipment.

Proof of qualifications

- Does the person standing here actually have the right qualifications, training or certificates and can we hold the company where this person works liable for this?

Proof that rules and laws are being followed

- Can the supervisory body or inspector verify whether everything is done according to the rules (compliance), both for inspections on the road and based on submitted documents?

The people or systems used to carry out the work act on behalf of the companies or supervisory bodies: the organisations are liable here rather than the people, with a few exceptions.

In many cases work is also outsourced, so a transport order may be subcontracted a few times. The driver who comes to collect a cargo may be self-employed and temporarily working for a small transport company, which in turn is engaged by a major logistics service provider, which performs the contract on behalf of the cargo owner. A service technician may be self-employed and engaged by a small service company, which is hired by a major service company to perform maintenance for an equipment manufacturer. There appears to be an increasing need for digital proof in these situations.

It would be useful if there were a way:

- For one party to provide robust (legal and practical) digital proof to the other party rather than having just hardcopy proof.
- To create a work process that suits (varied) practical situations, with changing and sometimes temporary staff who have little IT-related training and limited knowledge of systems and processes.
- To apply the solution broadly at acceptable costs.
- To create a free market for IT service providers who can offer these solutions in a competitive setting.

This document describes a generically applicable method that meets these conditions.

2 Digital proof

After 2010, a new standard for digital proof has gained popularity: the JSON Web Token or JWT⁶. Currently signed JWTs are used most frequently as proof between IT systems, between servers: they are a tried-and-tested way of sharing permissions and identities of users. The OAuth open standard, for example, is based on this technology. Its broad application means that support is available, such as software libraries in various programming languages.

The standard is flexible and more versatile than its current use would suggest⁷.

A signed JWT conforms to the JSON Web Signature (JWS) specification. A JWS is the general standard for transferring content with confidence (a document for example), whereas a JWT is specifically aimed at 'claims': the question whether identities can be trusted.

JWT: An application of a JWS that is specifically used for transferring **claims**. These are pieces of information (like a user ID, access rights or session details) that are used in authentication and authorisation systems. JWTs are widely used in Single Sign-On (SSO) solutions and for API access.

JWS: Designed to secure **general data** by adding a digital signature, which is used to guarantee the integrity of the data and the authenticity of the sender. They are widely used in situations where secure exchange of data is important.

This document uses JSON Web Signature (JWS) Unencoded Payload Option⁸, as this standard is better suited for embedding than the JWS standard⁹. The digital proof in a JWS consists of three interlinked parts:

- **Its content (payload)**
 - the claims being made by the sender;
 - possibly with additional data, such as a validity period.
- **Proof that the payload has not been changed since it was sent by the sender**
 - a hash or fingerprint^{9A}.
- **Proof that the payload plus the proof of 'being unchanged' has truly been sent by the sending party rather than by another party with a false identity**
 - signing ('encryption') using a recognised certificate that belongs to the sender.

The mathematical basis (cryptography) for this proof is widely known and used for important transactions almost everywhere on the internet. This type of proof is legally robust if its implementation is done properly. A proper implementation includes choosing the right version of the standard, setting the whole organisation up correctly and using the correct certificates.

⁶ [RFC 7519: JSON Web Token \(JWT\)](#)

⁷ *Verifiable Credentials and wallets are a possible alternative that could become widely accepted in the future. JWS is a compatible format.*

⁸ <https://datatracker.ietf.org/doc/html/rfc7797> RFC 7797 - JSON Web Signature (JWS) Unencoded Payload Option

⁹ <https://datatracker.ietf.org/doc/html/rfc7515> RFC 7515 - JSON Web Signature (JWS)

^{9A} [SHA-2 - Wikipedia](#)

High-quality certificates can be used for important data¹⁰ representing a large value. eIDAS certificates (sealed digital documents) are one example of this. When these certificates are used, 'signing' will meet the strictest requirements for electronic signatures¹¹.

The digital proof can be stored for an unlimited period: the three elements of payload, proof that the payload is unchanged and proof of who sent it will always apply. If anyone were to change the payload, this would be visible immediately.

There are a number of standard 'payload' definitions, but everyone is also free to define their own payload themselves. This offers lots of opportunities.

Digital proof for transport could, for example, have the following payload:

- The truck's registration number.
- The driver's name and ID number.
 - Any special certificates held by the driver, like for dangerous goods or safety training.
- Specifics of the cargo, addresses, etc.
- The digital identity of the transporter and the client.
- Proof that the client has issued the transport order to this transporter.
- The time and place of transfer.
- Additional documents.
- Photos.
- Etc.

2.1 Proof of identity and certificates separate

Note that in principle this digital proof does not replace someone's ID. The idea is for someone to have separate proof of identity or an ID card. The payload of the JWS is used to prove that the client is sending someone with a certain name and ID. A security guard can check the ID and compare it with the payload of the JWS. The person can then proceed if they match.

The standard for JWSs does allow modern digital identity and training certificates (verifiable credentials/presentations) to be included in the JWS, which renders the method future-proof⁹.

2.2 Proof inside proof: useful for outsourcing

The standard allows a complete JWS to be 'wrapped' as digital proof as part of the 'payload' of another JWS, like an envelope inside another envelope. There is basically no limit to the number of times this 'wrapping' can be done.

Wrapping proof in other proof is very useful for outsourcing. Take a transport order, for example:

- The first digital proof (JWS) could be the transport order: this transporter has actually been engaged by the seller to transport this cargo.
- This first JWS is wrapped in the next JWS: the digital proof that this driver and truck/registration was given the order to carry out the work on behalf of the transporter.

¹⁰ Examples are important waybills or bills of lading

¹¹ The EIDAS standard for adding electronic signatures to a JWT or JWS is relevant here:

https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.02.01_60/ts_11918201v010201p.pdf

In this way, single digital proof can be used to prove the order issuing chain¹².

The same applies to services: the order issuing chain is wrapped up in each other.

It is quite simple to specify that each JWS contains a link to the maker of the JWS. By following the link, you can verify in real time that the maker of the JWT still confirms that the JWS, and therefore the proof, is valid. Doing this step by step for each 'wrapped' JWS verifies the chain.

2.3 Flexible: last-minute changes

Creating a JWS requires relatively little time and computing power. These characteristics make it easy to implement last-minute changes when creating a JWS.

One example is if the initially assigned registration and driver need to be changed after all: putting a new payload in a JWS is very easy.

¹² Technically there are two types of solutions: including the whole signed JWS in another one or including only a link to the source of the JWS. Each one has its pros and cons. This description assumes that including a whole JWS in the "envelope" of another JWS is the more robust method.

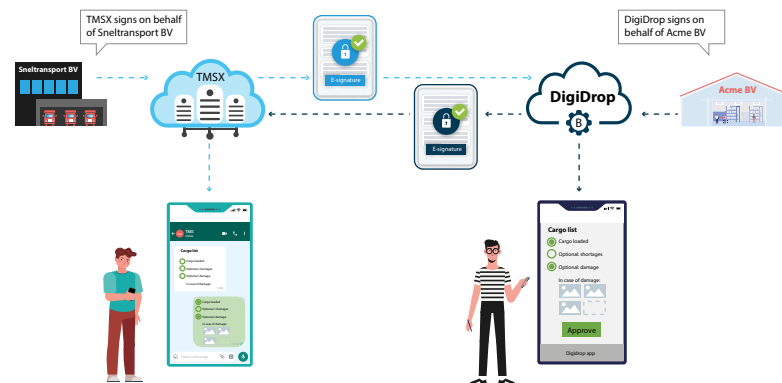
3 Application in practice: between companies

Even though these types of digital proof are widely known in the IT sector, this technology does require a good level of technical knowledge and professionalism of implementation and management. You need to have knowledge of digital certificates and be able to handle large types of digital proof.

How, then, can you still make them simple and easily applicable in logistics for people with hardly any IT training?

The inspiration for this can be taken from DigiD and the widely used 'Tikkie' application for small payments. They are easy to apply, while the complex technology behind them is managed by professional companies behind the scenes. People use well-known tools (app, chat, email, QR codes, links, their PIN) to close the chain.

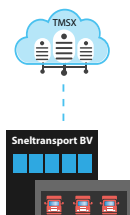
The major step forward here is that IT systems exchange 'electronic signatures' on behalf of their companies. They are (digitally) mandated to do so.



Electronic signatures between DigiDrop and TMSX on behalf of the clients

In this scenario, the people are not the ones 'signing' things. They are interchangeable 'operators' who add a small item of proof to the overall proof that the transfer is proceeding as expected. This overall proof may include things like:

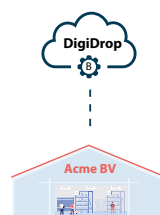
- The time.
- The location.
- The truck's registration number, the carrier's name or the driver's proof of ID.
- The shipment's identification.
- The device used by the warehouse employees, with additional properties such as its IP address, MAC address or other properties.
- The probability that the warehouse employee and the driver are in the same place at the same time and can see each other.
- A picture of the cargo.



Assurance

For TMSX and Sneltransport BV

- Identification of the DigiDrop entity
- Geolocation of devices and timestamp
- Order information
- Driver has met warehouse employee who performed the data check
- Driver confirms transfer
- Optionally photos and text
- Confirmation by Digidrop
- E-signature by DigiDrop



Assurance

For DigiDrop and Acme BV

- Identity of the TMSX entity
- Geolocation of devices and timestamp
- Order information
- Warehouse employee has met driver and performed the data check
- Warehouse employee confirms transfer
- Optionally photos and text
- Confirmation by TMSX
- E-signature by TMSX

This overall proof may be sufficient for the companies involved to have a transfer 'signed' by their IT systems. The legal basis for this is formed by the mutually agreed conditions.

This approach ensures that the IT systems of companies can add digital signatures based on a combination of proof that has been gathered. Human involvement is limited to an operational role in which they record data, but the actual 'signing' and validation are performed by computer systems. This system builds trust through:

- **Contextual data:**
Times, locations and ID-related data for objects, devices and persons.
- **Digital integrity:**
Techniques such as cryptographic signatures guarantee that the data remains authentic and unchanged.

The following description presents the version for the transport sector (called 'DigiDrop' in this document) in a simplified way. This version was developed for transferring goods in road transport daily practice¹³.

The version in the description tries to keep the requirements for the equipment on the shop floor to a minimum. It also takes into account practical obstacles (no connection in the warehouse for example) and fallback options¹⁴.

Providing proof of subcontracting, proof of professional certificates and proof to supervisory bodies all have almost identical functionality.

The description in this chapter is aimed at business interactions; the description for use by supervisory bodies has been removed and is presented in chapter 5.

¹³ To simplify the explanation, it covers only one of the technical versions that are possible. In the further specification, you can make an assessment of why you should prefer one version over the other.

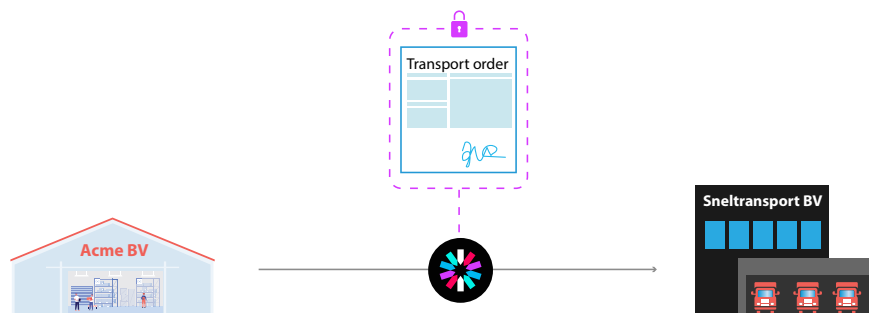
¹⁴ Annex 1 covers a few of the relevant considerations.

3.1 Basic DigiDrop

First of all, the basic version is explained, followed by the fallback options in case of an obstacle, like not having mobile internet in the warehouse.

The explanation uses the example of collecting goods from a warehouse. Delivery would be performed in the same way, only with a receiving employee and the recipient.

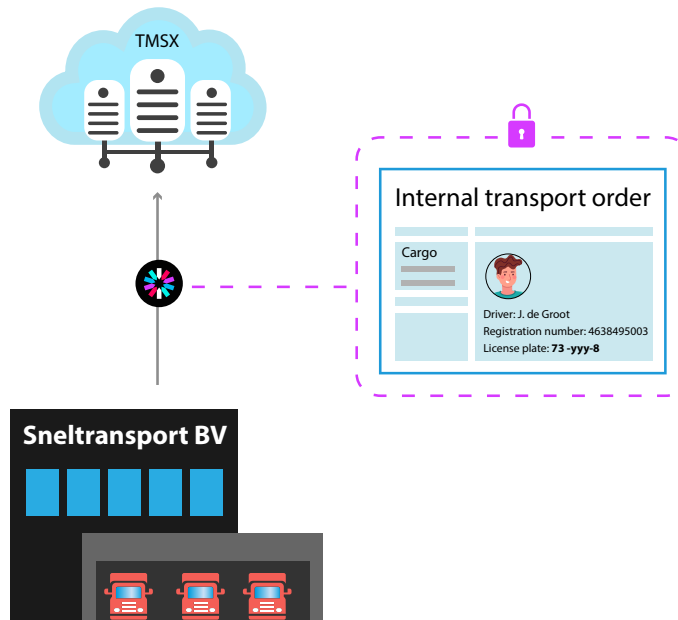
A trading company (Acme BV) has sold a few pallets of goods and issues a digital transport order to Sneltransport BV. This is also done in the form of digital proof (JWS, signed by Acme BV).



Acme BV sends digital proof of the transport order to Sneltransport BV

Sneltransport BV makes use of the Transport Management System (TMS) TMSX, creating an internal transport order: the driver and truck's registration number are now present in TMSX.

At the start of the relationship, Sneltransport BV issued digital proof to TMSX that TMSX may act on behalf of Sneltransport.

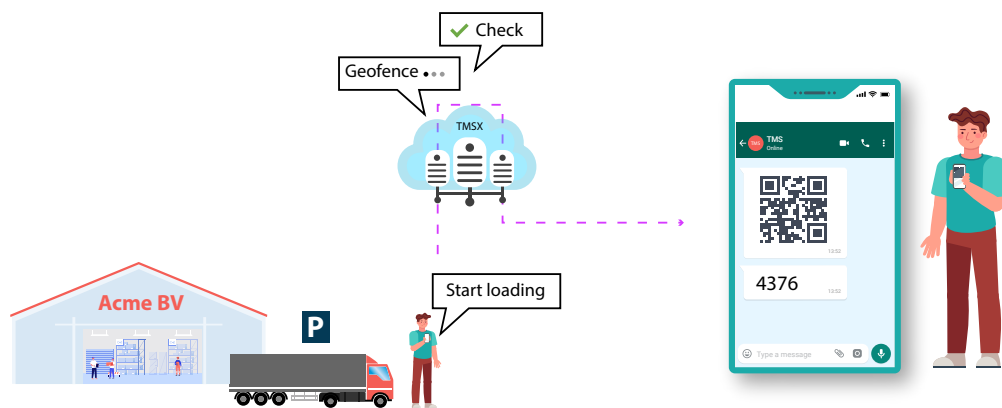


The digital proof of the transport order is present in TMSX

The driver has a mobile phone with WhatsApp: the driver's number and identity (including their ID number) are present in TMSX.

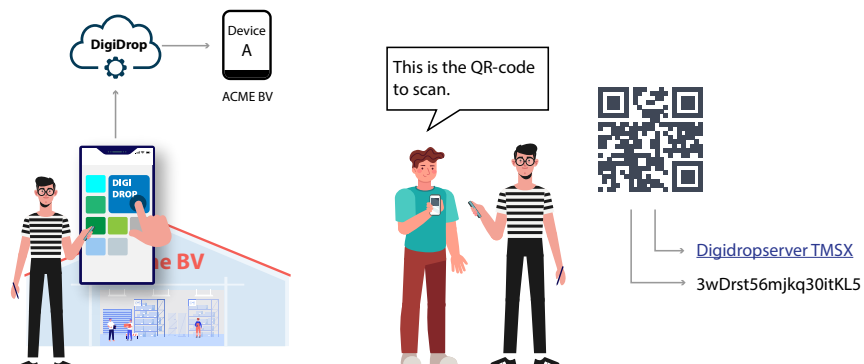


The driver takes the truck to the Acme BV warehouse, parks it, notifies TMSX that they will start loading and reports to the warehouse to collect the pallets.



TMSX verifies the geolocation of the phone and the truck: they must be in the vicinity of the known address. TMSX sends a temporary QR code and a temporary PIN to the driver via WhatsApp.¹⁵

The Acme BV warehouse employee has a registered phone or a company tablet. This will be registered with Acme BV's DigiDrop provider (a new role) as belonging to Acme BV. The DigiDrop provider's app is installed on the phone.



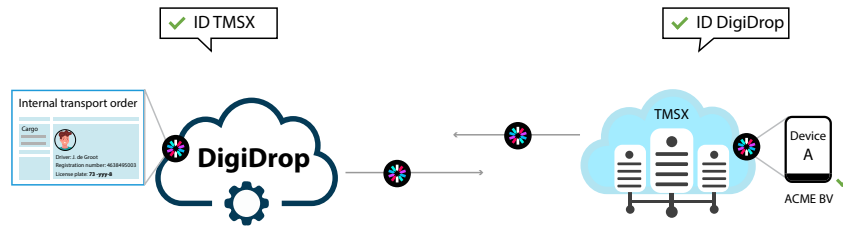
The warehouse employee scans the QR code using the app. The QR code contains:

- A link to TMSX's DigiDrop server.
- A unique temporary code for this transfer.

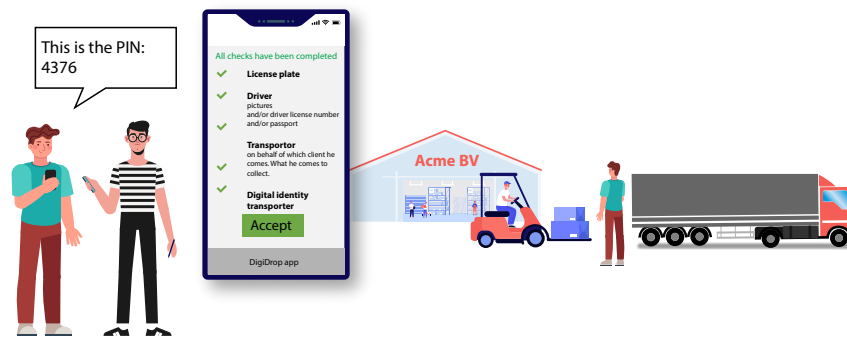
¹⁵ To clarify the explanation, the PIN and QR code are presented in a single image. In practice these will be supplied separately.

Acme's DigiDrop provider and TMSX then start performing the technologically complicated work of:

- Verifying each other's identity.
- Exchanging digital proof of representation (TMSX on behalf of Sneltransport, the DigiDrop provider on behalf of Acme BV).
- TMSX sends the JWS to DigiDrop, which verifies the proof: has it been signed? Is it unchanged?
- The payload is extracted and viewed, and verified against other information.
 - Do the details match the location, identities and internal orders?



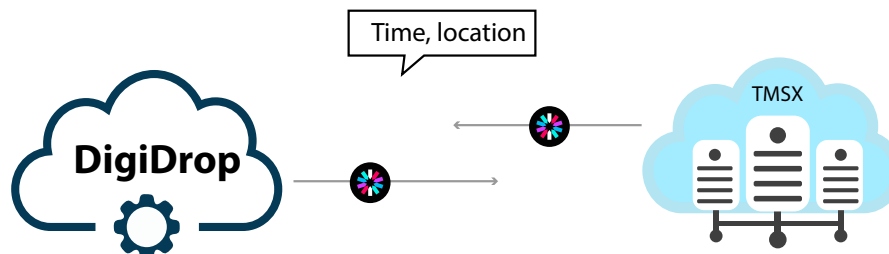
If this is all satisfactory, the warehouse employee will be asked to 'enter the PIN': this is the PIN the driver received via WhatsApp. The driver passes it on to the warehouse employee¹⁶.



After entering the PIN, the warehouse employee can see the necessary details in the DigiDrop app, such as:

- All checks have been completed.
- Registration, driver ID, transporter.
- The sales order.
- The cargo being collected.

The warehouse employee confirms the details in the app, after which the cargo can be loaded.

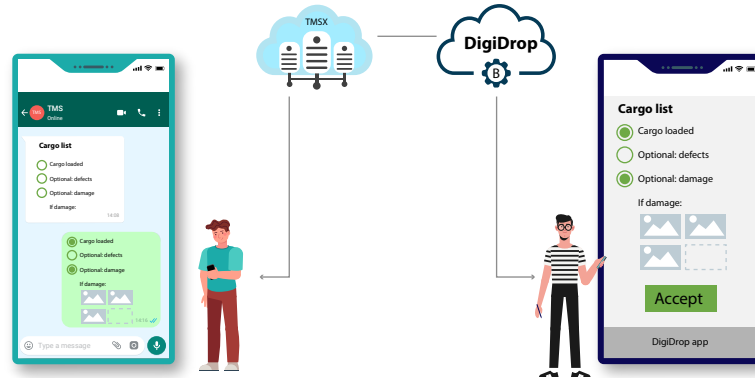


The DigiDrop provider and TMSX exchange the digital proof of the confirmation (time, location, etc.)¹⁷

¹⁶ The PIN adds little in terms of proof, but it does create a barrier to showing privacy-sensitive data. By giving the PIN to the other employee, the driver basically grants permission for them to view the data, including their name, driving licence or other data.

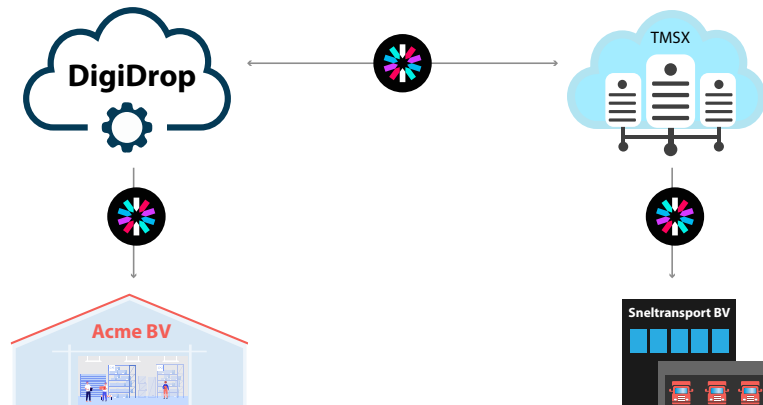
¹⁷ The DigiDrop provider creates and signs a JWS, which is sent to TMSX.

After loading the cargo, TMSX sends the cargo list to the driver's WhatsApp once again, asking whether there are any comments, defects, damage or changes. If so, the driver will submit those, possibly with pictures as proof.



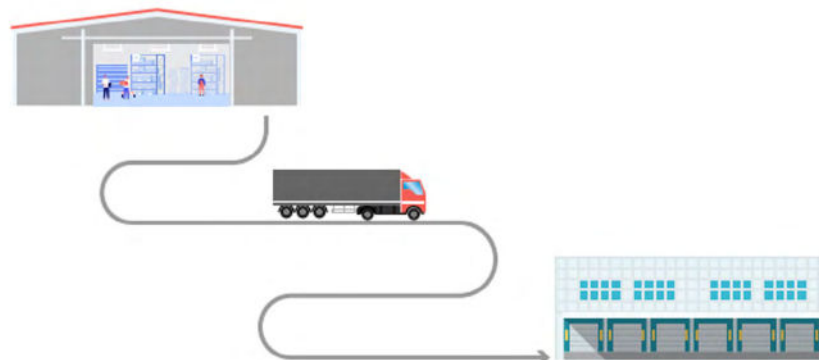
TMSX sends the cargo list with the comments to the DigiDrop provider

In turn, the DigiDrop providers shows those extra details/comments/pictures to the warehouse employee in the app for approval. The warehouse employee approves this via the app.



*The DigiDrop providers sends TMSX signed digital proof of the approval.
The DigiDrop provider forwards the same proof to Acme BV for their records.
TMSX forwards the proof to Sneltransport BV for their records.*

The driver can then leave and drive to the delivery address.



3.2 Obstacles

No mobile internet in the warehouse

Generally speaking, the warehouse employee will be able to use internal Wi-Fi, but the driver will not. If the warehouse contains lots of metal, the driver may not be able to connect to their mobile internet inside the building.

As TMSX sends both the QR code and the PIN to the driver beforehand, the lack of connectivity should not be a problem for the transfer.

After loading the cargo, the driver does need connectivity to forward any defects, comments and pictures, but taking the pictures does not require internet.

The mutual approval of the comments does not require the driver and the warehouse employee to be in each other's vicinity: they can do so separately.

The warehouse employee cannot scan the QR code

Some devices have no camera or cannot scan a QR code.

The alternative is for the driver to receive a unique short URL in WhatsApp. This URL can be copied quite easily. There are many kinds of service providers who supply URL shorteners. TMSX could use one of these to have a long specific URL, which would be found in the QR code, converted into a short unique (and temporary) URL.

The warehouse employee's device is broken or has no connection

In this case, the solution would also be to use a short URL. The warehouse employee can then write the short URL down on paper to use it later or to call someone with a PC and a browser, who can then use the URL to contact the DigiDrop provider. This person can check the details remotely.

TMSX is temporarily unavailable

If the driver already has a QR code (or short URL) and a PIN, the warehouse employee will in any case be able to copy these. It would then be up to the parties to find a solution, probably using a phone and paper.

3.3 A warehouse does not have a DigiDrop provider

What if the driver arrives at a warehouse where the employees do not have devices with a DigiDrop provider app and do not have a subscription with one of these providers either?

In that case you have a fallback option, which may be less secure and reliable but still workable, as long as the warehouse has devices with a browser and an internet connection.

The driver receives a temporary PIN and a short URL in WhatsApp upon arrival. (A QR code can obviously also be used if the warehouse employee's device can read it.)

The warehouse employee uses this short URL in a browser to connect to TMSX. The PIN is used to view the information. The details can be forwarded by email or downloaded.

After loading the cargo, the dialogue between the warehouse employee and TMSX is resumed in the same browser.

This version is less secure than using a DigiDrop provider, as TMSX needs to be fully trusted by the warehouse. In practice, however, it will be an acceptable fallback option in many cases.

3.4 Inclusion in general terms and conditions

The legal basis will be strengthened if the two parties involved include this working method in their general terms and conditions, i.e. that this way of working is acceptable as proof of transfer (commercially speaking, under civil law).

The seller should include this in its general terms and conditions for delivery to customers.

The transporter should include this in its general terms and conditions for delivery of the transport order.

The seller has a contractual agreement with the DigiDrop provider (or arranges this themselves), describing the working method and requirements.

The transporter has a contractual agreement with TMSX, describing the working method and requirements.

In turn, the recipient also has a contractual agreement with another DigiDrop provider (or arranges this themselves), describing the working method and requirements.

4 Method for proving training and professional certificates

The payload of the JWS can be a description of a certain training or professional certificate. A professional driver, for example, may have both a truck driver's certificate and an endorsement for dangerous goods. A service technician may have a certificate stating that they are allowed to work with heat pumps and refrigerants, etc.

By standardising these descriptions, you can prove both beforehand and afterwards that the creator of the JWS (the liable organisation) has made this statement: the person that was sent has the necessary 'papers'¹⁸.

In the not-too-distant future, digital proof of these training or professional certificates will become available: so-called 'verifiable presentations' of 'verifiable credentials'. Embedding this digital proof of certificates in the JWS will provide even more security.

'Verifiable credentials' (abbreviated to VC) are now usually a digital version of a document that used to be hardcopy. Initial applications are things like airline tickets, known as boarding passes stored in the wallet on your phone. Governments are busy developing similar solutions for digital driving licences and digital IDs.

A VC can also serve as digital proof of something less tangible, like having a bank account. An issuing institution (bank, government, training institute, etc.) provides a VC digitally signed by them to a 'holder', e.g. a service technician who holds a particular certificate. The technician can show the VC to someone who wants to know for sure that the technician has that specific certificate. The trust is based on the issuing institution's reputation.

In business applications, it is important to realise that the company is liable rather than the person. The person uses VC to prove to the company employing them that they have a valid certificate; the company uses the JWS to prove to the customer that they are following the agreements, i.e. are using a qualified person.

¹⁸ A person can show a hardcopy document to the company as proof. The company provides the customer with digital proof to guarantee that this person is qualified. In other words: part of the chain may still consist of hardcopy documents, as it does make the system easier to introduce.

5 Application in practice for supervisory bodies

Chapters 3 and 4 outline applications involving commercial interaction between companies.

It turns out that the same mechanism can be used for supplying data to supervisory bodies. The eFTI Regulation will be providing a solution for part of the data required by supervisory bodies.

This document contains a proposal to:

- Apply the same technology (JWS) that is suitable for commercial business interactions.
- Choose a generic mechanism that is basically suitable for all types of proof.

5.1 Open four corners model for inspections

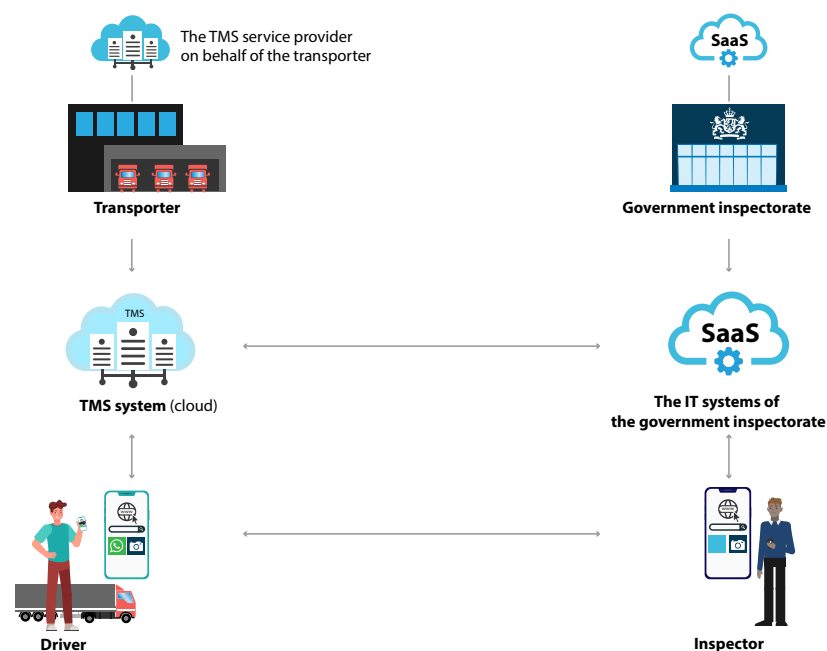
The number of laws and regulations relating to goods transport is considerable: some of them are about the means of transport and the driver (safe professional transport according to the rules, dimensions and weights, emissions, driving and resting times, etc.), but most of them are about the goods themselves (levies, dangerous goods, perishable goods, foodstuffs, products of animal origin, etc.).

Government services that supervise compliance with these laws require data in order to carry out their duties, from data in formal notifications provided in advance to insights into documents and data in IT systems during (physical) inspections, both during and after transport.

The provision of data to an inspectorate can be schematically described as an open four corners model; it is open because the participants in the four corners are not restricted to a limited group.

The four corners are formed by:

- The TMS service provider on behalf of the transporter.
- The driver on behalf of the transporter.
- The IT systems of the government inspectorate.
- The inspector who conducts the physical inspection.



The basic assumption is that the employees who act on behalf of their organisation have smartphones or tablets with connectivity (usually continuous, but not always): mobile internet or company Wi-Fi.

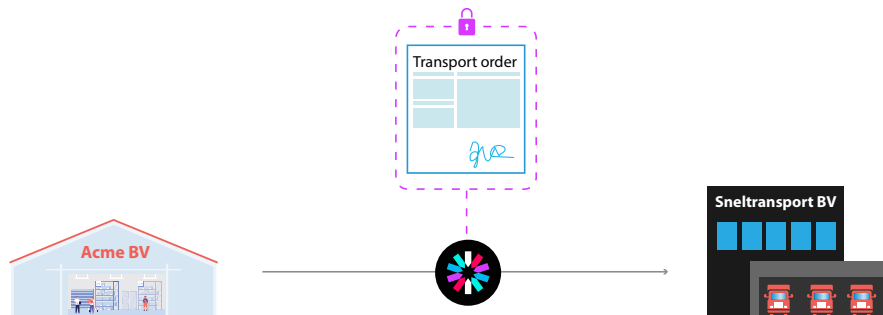
The driver has a smartphone that is registered with the TMS provider: SIM card, MAC address, etc. The lowest possible barrier is to use WhatsApp or another standard chat application for the interaction between the TMS and the driver.

The inspector has a mobile device that is registered in the inspectorate's IT system. The inspectorate's application is installed on the device.

5.2 Providing proof to an inspector

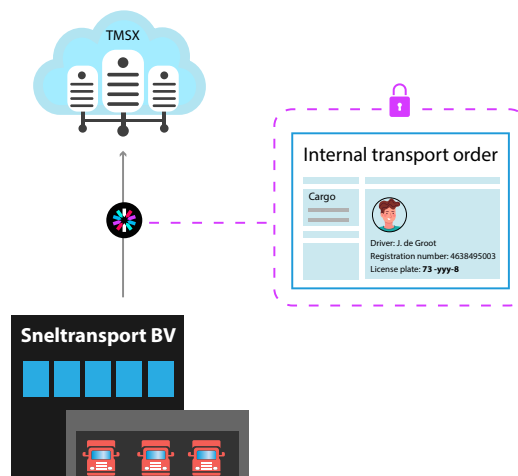
The explanation uses an example with one shipment.

A trading company (Acme BV) has sold a few pallets of goods and issues a digital transport order to Sneltransport BV.



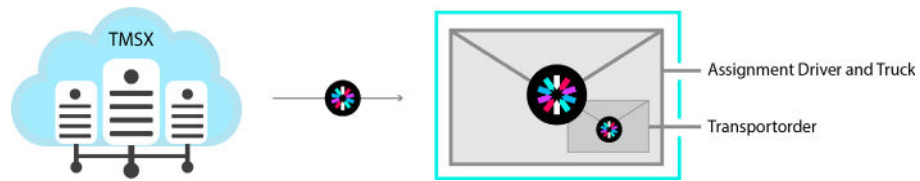
Acme BV sends a JWT with the order information to Sneltransport BV.

Sneltransport BV makes use of the Transport Management System (TMS) TMSX, creating an internal transport order: the driver and truck's registration number are now present in TMSX.



TMSX receives the Acme JWT from Sneltransport BV.

The driver has a mobile phone with WhatsApp: the driver's number and identity (including their ID number) are present in TMSX.

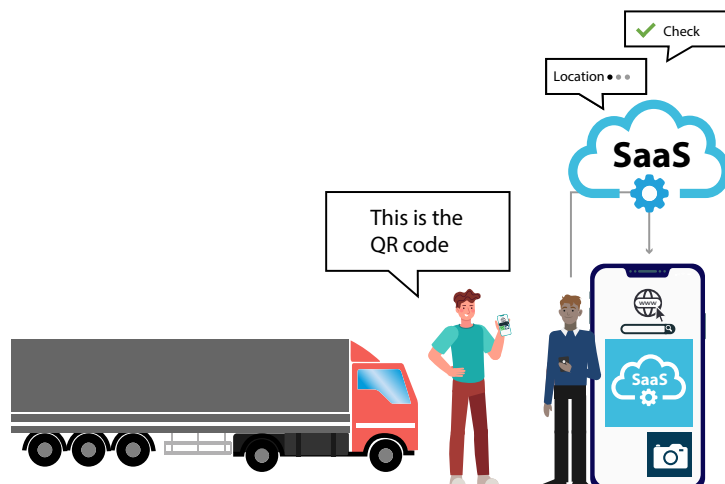


TMSX creates signed proof using the Acme JWS, the proof of representation from TMSX on behalf of Sneltransport BV and additional information about the truck and the driver.

The driver goes to the Acme BV warehouse, collects the cargo and starts the journey. During the journey, an inspector stops the truck and asks for details. The driver notifies TMSX that there is an inspection.



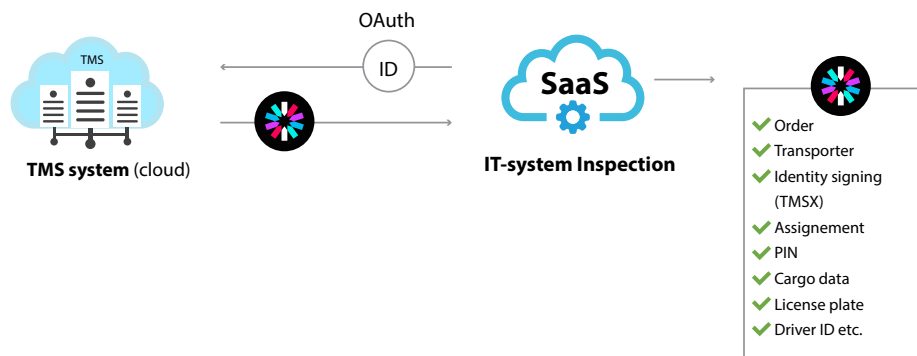
TMSX verifies the geolocation of the phone and the truck: they must be in each other's vicinity. TMSX sends a temporary QR code (or a short URL that can be copied) and a temporary PIN to the driver via WhatsApp. The QR code provides the identity of TMSX and the link to the TMSX servers, combined with the unique identifier for this interaction.



The inspector scans the QR code using their device and the inspectorate's app.

The inspectorate's IT system verifies:

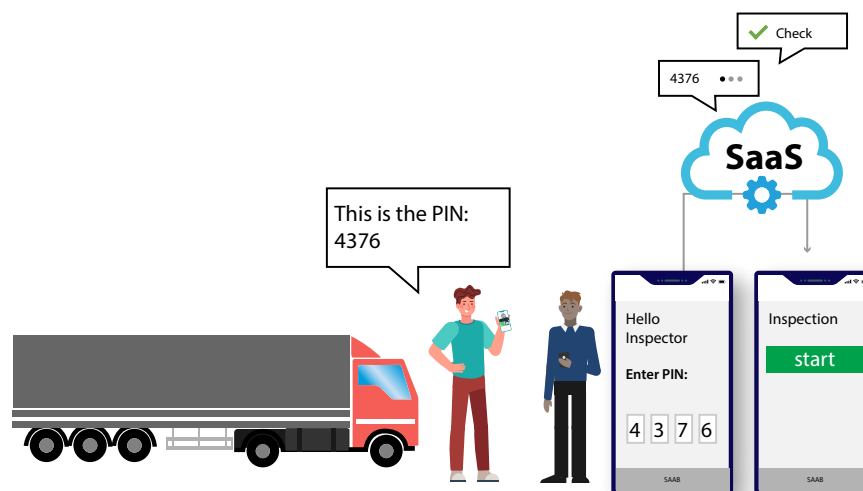
- The inspector's device location/IP address.
- The TMSX identity (digital).
 - Whether the party is known and certified.



The inspectorate's IT system identifies itself in TMSX and requests the JWS in question.

The inspectorate's IT system assesses the JWS:

- Checking of order information and shipment.
- Checking of transporter.
- Checking of identity signing (TMSX).
- Checking of order issuing (who engaged the transporter).
- Extraction of temporary PIN, cargo details, registration, driver ID, etc.



The inspectorate's IT system asks the inspector for the temporary PIN, which the driver needs to enter. If this is correct, only then is the information shown in the inspector's app for security and privacy protection.

The inspector can then conduct an inspection.

In this example, the transporter may have come from any country: as long as the inspectorate's IT system and TMSX trust each other's digital identity, the transaction will work.

The inspectorate's IT system has the same data as the inspector and can immediately process and save the results of the inspection.

A notification to the inspectorate can be made in the same way, separately from an inspection on the side of the road.

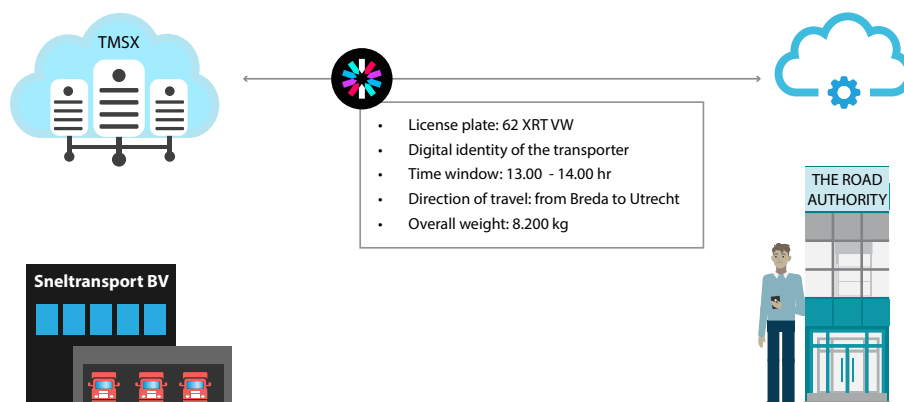
5.3 Broader usage: privileges

Verifiable digital proof can be used more broadly, for example, to allow and check privileges as described in the example below.

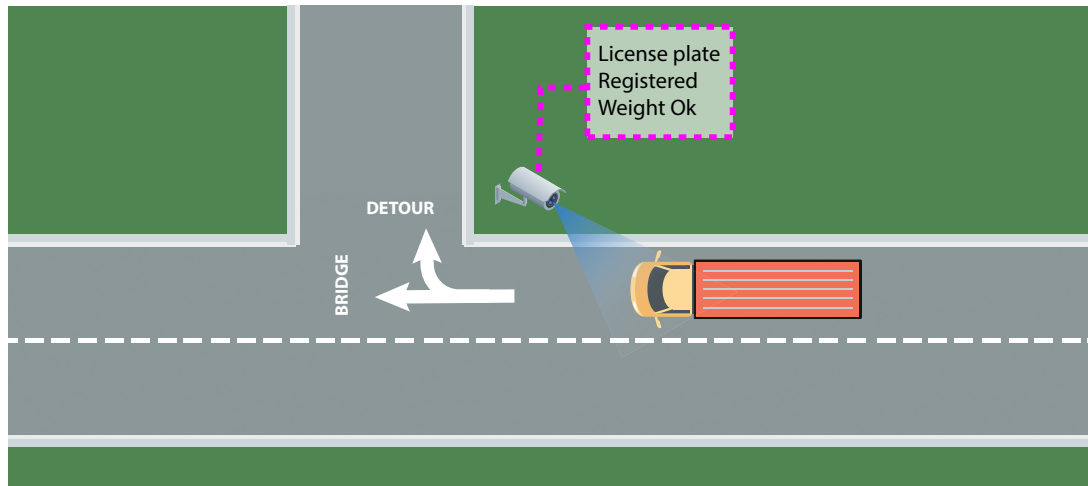
One of the bridges in the road network appears to have defects. The road authority imposes a temporary weight restriction for goods traffic until repair work can start. Empty or almost empty trucks should in principle be allowed to cross the bridge, but heavily loaded trucks are banned.

The procedure is for TMSX to send digital proof to the road authority on behalf of the transporter half an hour or more in advance, stating:

- The truck's registration number.
- The digital identity of the transporter responsible.
- The time window in which the bridge will be passed.
- The direction of travel.
- The declaration of overall weight (under the limit).



The road authority has installed an access barrier for trucks in front of the bridge, where an ANPR (licence plate recognition) camera scans the registration numbers. A registration that matches a previously accepted declaration that is still valid may pass, unless it is decided to perform a random inspection. Unknown registrations, registrations with invalid proof or trucks that will be inspected must park on the side.



When a known registration has passed (or its validity has expired), the digital proof is archived and the exemption is withdrawn; this prevents the system from being abused. Transporters who abuse the system may be added to a blacklist. TMSX may submit digital proof, but the declaration may be rejected based on the identity of the transporter (and/or the registration).

This example shows that a (wrapped) JWS is a broadly applicable mechanism.

6 Market forces

The JWS specification is an open global standard that can be freely applied by anyone. The software libraries for handling JWSs are freely accessible.

The use of certificates such as eIDAS is readily accessible as such for any professional party.

The open publication of agreements on payload and processes removes any barriers for parties to implement things themselves.

Considering past experience with JWSs in current practice, it can be assumed that implementing and maintaining IT equipment for this system will be easy and affordable. In practice, general IT suppliers, platforms, specialised service providers and government IT services will make their own choices on implementing these kinds of solutions themselves or purchasing a service from a SaaS party.

7 Support by the Basic Data Infrastructure

The Basic Data Infrastructure (www.bdinetwork.org) supports the working method described above in various ways.

7.1 Trust in parties

The issuer of a digital certificate (eIDAS, etc.) used to digitally sign a JWS guarantees the relationship between a legal entity (company, institution, government service) and the certificate. This relationship ('the party that added this digital signature is actually this party') is about identity rather than the (commercial) trust in the party.

The BDI Association is a local decentralised legal entity that supports its members in building up mutual trust and trust in third parties. The local register links identity to trust: <https://bdinetwork.org/deployment/governance/>.

If governments and companies want to introduce this (JWS based) working method, it would be nice if you could verify whether the other party is following the agreements. By ensuring that all parties become members of a BDI Association, sign the rules and pass a few tests of the technology beforehand, you can verify in real time whether you are dealing with a 'certified' party.

This real-time check makes use of what is called the Association Register, maintained by the Association.

7.2 Shared general terms and conditions

Paragraph 2.4 mentions the usefulness of shared general terms and conditions, specifically written for this application. In BDI terms these are called Edge Agreements: <https://bdinetwork.org/interoperability/edge-agreements/>.

Members of a BDI Association can mutually agree on these terms and conditions, which creates a sound legal basis. It is cheap and convenient to arrange things this way.

7.3 Shared semantics

The payload of digital proof has a lot of freedom: while this is useful, it can be technically difficult for its application if you have no agreements on terms and meanings.

The BDI framework assumes that there will be subtle local differences in definitions, which will depend on the sector, language, culture and local legislation: <https://bdinetwork.org/framework/core-principles/core-principle-6/>.

A BDI Association (or a group of BDI Associations) makes its own agreements on standards in this regard.

7.4 Shared services

If members are willing to pay for it, a BDI Association can provide a number of services for them to share the costs or to share expertise. Examples of this are the 'DigiDrop provider' service or a register of persons' mandates.

8 Hybrid working methods

The BDI framework takes into account the fact that in reality quite a few parties in an (international) chain are not yet properly digitalised. Sometimes they are unable (financially or in terms of expertise) to implement modern IT systems, and sometimes they do not trust the system. Data sharing and data integration provide greater transparency, but not everyone recognises its advantages.

In the transport sector's daily practice a larger transporter will often engage a charter through an intermediary, and sometimes that work is subcontracted again, which is invisible to the transporter. As far as the transporter is aware, the transport order has been issued and a while later a hardcopy waybill will be submitted as proof that the order has been handled. If a client calls to report that no driver appeared at the agreed time, the transporter will have to call the intermediary to find out what happened.

Signing off transfer moments (loading, unloading) would already be a major step forward, and it would be even better if digital messages were being sent regarding delays or other problems. But how can that be arranged without apps, DigiDrop providers or data integration?

Two possible working methods are described in the following. These methods are examples of what are called 'Edge Agreements' in the BDI framework: hybrid working methods to bridge that gap to the 'not-so-digital' reality.

The first method described has been made as simple as possible, but does produce digital events for everyone involved: loading in and delivery.

The second one has a few more options, but also requires more from the users.

8.1 DigiDrop UltraLite Edge Agreement

TMSX is the TMS system used by the main transporter. The transport orders to be outsourced are created in TMSX.

TMSX generates three unique codes for each shipment, each consisting of 4 letters:

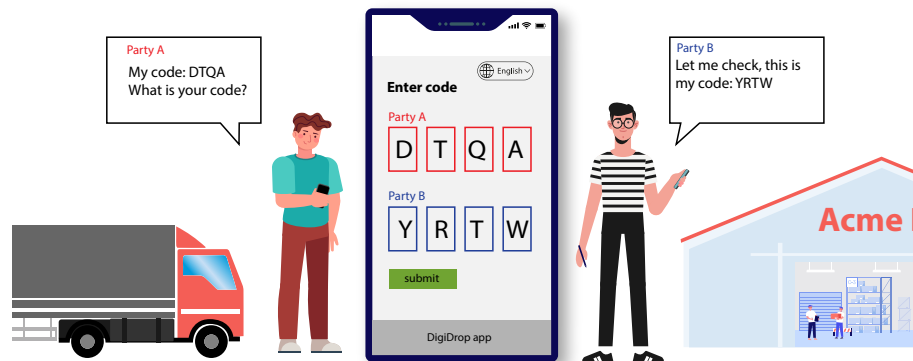
- E.g. 'DTQA' for the charter with the transport order for the shipment. The charter sends the order and the code to the driver.
- E.g. 'YRTW' for the warehouse where the shipment will be loaded up.
- E.g. 'PGHF' for the receiving customer, linked to the shipment/order.

TMSX sends the two combinations (DTQA+YRTW and DTQA+PGHF) to the www.digidrop.online website with a link back to TMSX. TMSX has all the data, the website is just an easy standard way for users to enter the codes.

The transport order is handed to the charter using a (hardcopy) CMR.

When the driver arrives to collect the shipment, either the driver or the warehouse employee will open the www.digidrop.online website, preferably on a mobile device.

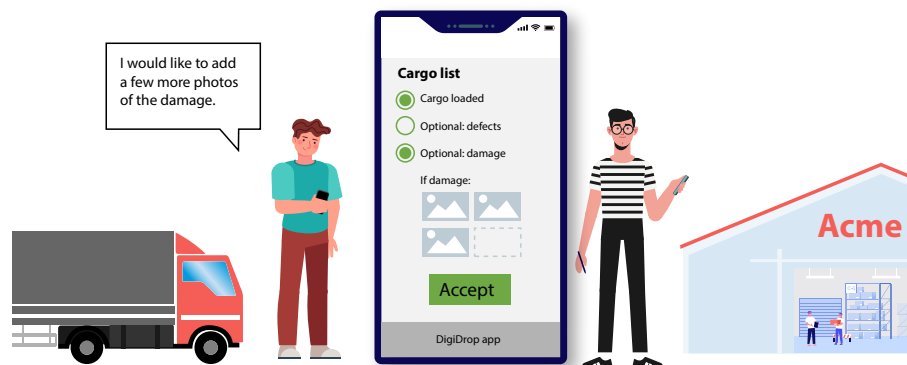
Here they each enter their 4 letters, making a total of 8. (DTQA YRT)¹⁹.



The website uses these 8 letters to recognise the shipment, the step in the process and the fact that TMSX is the party handling the order.

TMSX shows a few details of the order as a means of verification.

In its most minimal form, the transfer is reported at the press of a button. A somewhat more elegant version has the option to add comments and pictures (on a mobile phone).



TMSX can then digitally report to the clients that the shipment has been loaded.

The process is identical when the shipment is delivered to its destination.

The advantages of this approach are:

- The code can be written down and handed over on paper if required.
- Intermediaries and charters who do not trust the system will not 'leak' any sensitive information.
- The transfer moments become digitally available in real time.
- The process works in parallel to hardcopy waybills.

¹⁹ It is easy to deal with the codes being switched

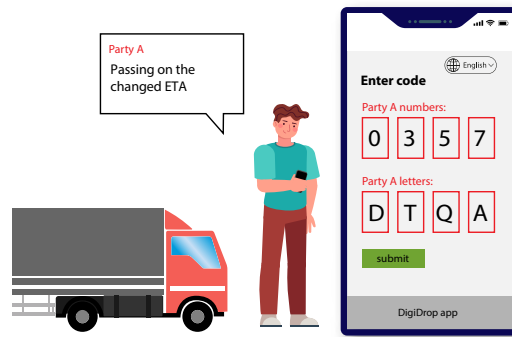
8.2 DigiDrop Lite Edge Agreement

A relatively simple expansion can add greater digital visibility about the progress of the process and planning.

TMSX will now generate three unique codes, each consisting of 4 numbers and 4 letters:

- E.g. '0357 DTQA' for the charter with the transport order for the shipment. The charter sends the order and the code to the driver.
- E.g. '0668 YRTW' for the warehouse where the shipment will be loaded up.
- E.g. '0890 PGHF' for the receiving customer, linked to the shipment/order.

While on the road, a driver can use the code '0357 DTQA' on www.digidrop.online to send messages about things like delays and a new ETA.



Entering the code '0357 DTQA' on the website gives you simple dialogue options, like entering 'new arrival time 16.30 - 18.30 hrs' in a text field. This is 'safe' for distrusting parties, because nothing will leak about who is making these changes.

TMSX will receive the update and can forward it digitally.

The warehouse or receiving customer can use the same process to retrieve information: entering 4 numbers and 4 letters shows the shipment's status.

The transfer is reported in the same way as for the UltraLite version: entering 2 x 4 letters and signing off.

This example shows how a hybrid process can be designed to bridge the gap between the world where the benefits of data integration are utilised with mature IT systems and the parties where IT integration is not yet quite so developed.

Annex 1: JWSs and QR-codes

In the working method described, the driver receives a QR code, which mainly consists of a unique link (in this case) to TMSX.

In principle, it would also be conceivable for the driver to have the whole JWS with them on their device. However, QR codes are limited by how much data can be wrapped in them. JWSs wrapped up in one another quickly increase the amount of data, easily exceeding the limit of what can still be realistically done with a QR code in everyday practice.

In principle, other transfer methods should be usable in that case: NFC or Bluetooth transfers do not have that limitation. The downside of this is that it requires much more from equipment and personnel to ensure that the data transfer is reliable.

A JWS with links to other 'embedded' JWSs is much smaller and should fit in a QR code. The downside of this option is that verifying the JWT requires many more online checks with all kinds of parties.

One of the advantages of having a QR code with only a unique link is that it can be copied onto paper as a short URL, which is useful if anything goes wrong.

The choice of transferring only a link in a QR code shifts the bulk of the complex IT interactions to professional parties 'in the cloud', which improves convenience and robustness on the shop floor.

Annex 2: Relevant IT standards

The JSON Web Signature (JWS) ([RFC 7515 - JSON Web Signature \(JWS\)](#)) describes how a generic payload can be digitally signed and transferred in JSON format.

The JSON Web Token (JWT) ([RFC 7519: JSON Web Token \(JWT\) RFC 9493 - Subject Identifiers for Security Event Tokens](#)) describes the specific version of a JWS for sending 'claims'. Claims are primarily aimed at trusting identities.

As commonly used Base64 encoding has its downsides, especially when embedding JWSs and for large payloads, there is a version of a JWS that circumvents these downsides (<https://www.rfc-editor.org/rfc/rfc7797.html>).

For large payloads like pictures, it is better not to embed the pictures in the JWS: only the hash and an identification are included in the JWS, and the picture is attached.

The ASiC - EN 319 162-1 v1.1.1 (https://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf) ETSI standard standardises ZIP files for combining these so-called detached signatures with their hashed documents.

Within the European domain, JWT fields have been standardised for e-signatures and e-seals, among other things, for identifying the signer in question

(JAdES - TS 119 182-1 v1.2.1:

https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.02.01_60/ts_11918201v010201p.pdf)

Trustlist that can be used to verify certificates are:

<https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls>

<https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tc-tl>

The approach is compatible with basic principles as set forth by the Trusted Information Partners network: <https://www.trustedinformationpartners.nl/algemene-basisprincipes-en-functionaliteiten-open-ter-consultatie/>



BDI, Topsector Logistiek & DIL

Ezelsveldlaan 59 | 2611 RV Delft | +31 15 251 65 65

www.bdinetwork.org | www.topsectorlogistiek.nl | www.datainlogistics.org

