

Memo

To Herman Wagter
From Walter van Holst
Date December 20th, 2024
Project BDI
Subject Proof as provided by JWT/JWS

Introduction

In the context of the BDI programme which aims to provide a toolbox/set of standards for digital services replacing paper documents in intermodal and international logistics chains for use by all actors involved in these logistics chains (including shippers, transport companies, stevedoors, as well as senders and recipients of freight). A specific matter for this is the extent to which digital documents or messages and provide sufficient proof of certain events and/or attest authority or competence for actors in these logistics chains.

The main scenarios intended for this are:

1. Representation: e.g. a lorry driver does represent a shipper that has been contracted to collect/deliver a load;
2. transfer of cargo: proof of receipt or release of the possession of a load;

This memo is structured along the following lines:

- A general outline of JWT/JWS technology;
- A general outline of digital signature rules;
- Application of the above to the scenarios outlined in this introduction.

Outline of JWT/JWS technology

A JSON Web token (hereafter: JWT) is a specific implementation of the JSON Web Signature, and a standardised way to use the so-called JSON format (JSON is an abbreviation for JavaScript Object Notation) to describe claims about the provenance and contents of electronic messages (including calls to web-APIs). A JWT consists of three parts:

- Header;
- Payload;
- Signature.

The signature part uses, in the BDI-context¹, asymmetrically encrypted cryptographic hashes. These hashes are calculated based on the payload and/or the document the JWT contains a claim about. As a result of this, any change to the payload and/or the document will result in a discrepancy with aforementioned hash since the new corresponding hash can only be replaced by the owner of the private key with which the signature has taken place. Verification of the signature is possible since the cryptographic hash can be decrypted using the public key of the issuer and comparing it with the signed content.

In the BDI framework this JWT or a similar digital structure (JWS) is used with so-called “private claims” as payload. These private claims are statements which are relevant in logistics supply chains interactions between entities. The JWT/JWS technology can be used as-is for the purposes but a functionally similar method can be designed.

Digital signature rules

The relevant legal framework in the Netherlands is:

- Dutch Code of Civil Procedure (*Wetboek van Rechtsvordering* hereafter: Rv);
- Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (Regulation 910/2014/EU, hereafter: eIDAS Regulation, amended by Regulation 2024/1183/EU, hereafter: eIDAS 2.0);
- Dutch Civil Code (*Burgerlijk Wetboek* hereafter: BW).

Also relevant is the jurisprudence on electronic signatures (case references of Dutch judgments are in Dutch):

- ECLI:NL:HR:2019:957, Hoge Raad, 14 juni 2019, <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:HR:2019:957> ;
- ECLI:NL:RVS:2019:3356, Raad van State, 8 oktober 2019, <https://www.raadvanstate.nl/uitspraken/@117940/201902201-1-v3/> ;
- ECLI:NL:RBROT:2022:3242, Rechtbank Rotterdam, 18 maart 2022, <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2022:3242> ;
- ECLI:NL:RBROT:2023:10194, Rechtbank Rotterdam, 1 november 2022, <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2023:10194> ;
- ECLI:EU:C:2024:253, Court of Justice of the European Union, March 21st 2024, Case C-76/23, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62023CJ0076> ;
- ECLI:NL:HR:1993:ZC1148, Hoge Raad, 19 november 1993, NJ 1994, 622;

¹ The intended use of JWTs in BDI can be found at <https://bdinetwork.org/wp-content/uploads/2024/05/2024-BDI-Embedded-JWT-as-Representation-Evidence.pdf>

Scenarios

1. Representation

In the context of BDI the intended application of JWTs is for attestations of contractor-subcontractor-relationships in logistics. A typical use case would be:

- A shipper contracts a haulier;
- Haulier contracts a subcontractor;
- Subcontractor arrives at the gate of the shipper. Shipper requires assurance that this particular subcontractor has been contracted by the haulier.

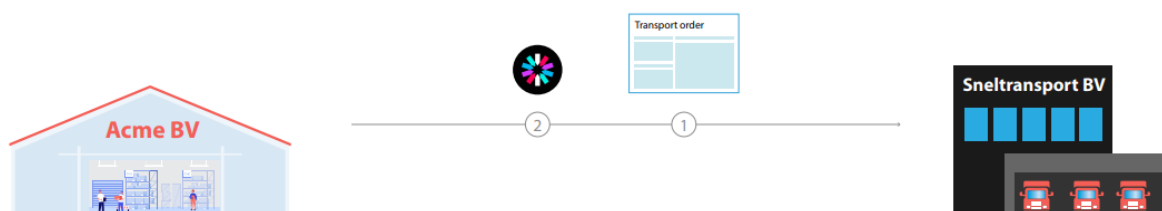
In the current (“paper”) way of working this would be solved by a bill of lading (with handwritten signature) that has the following characteristics:

- Proof of the transport agreement;
- Proof of receipt and delivery of the goods by the haulier;
- Proof of the visible conditions of the goods;
- Information carrier about the goods to be transported.

For the purposes of BDI the proof of the existence of the transport agreement and the proof of the subcontractor having been authorised to pick up specific goods are the relevant characteristics here.

2. Transfer of cargo

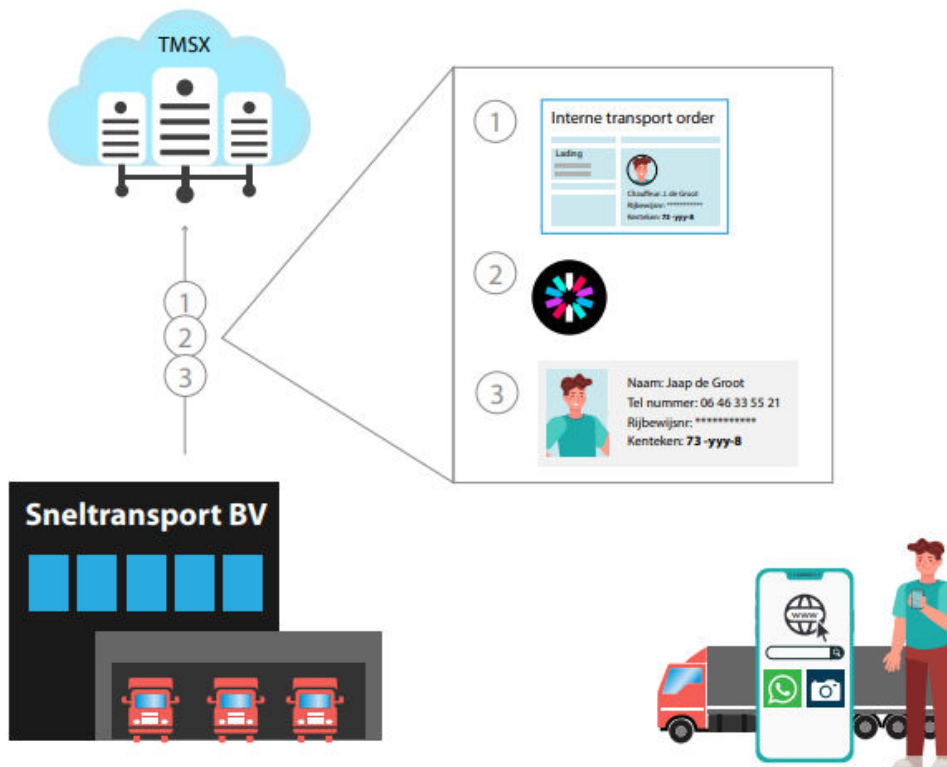
A trading company (Acme BV) has sold a few pallets of goods and issues a digital transport order to Sneltransport BV. This is also done in the form of digital proof (JWT, signed by Acme BV).



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

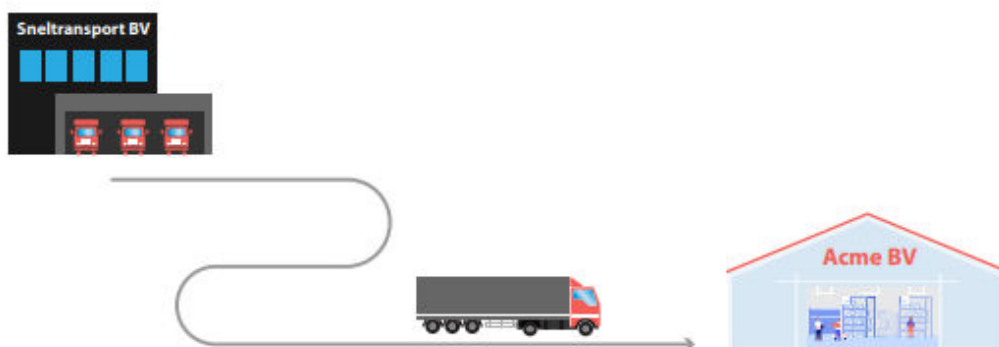
Sneltransport BV makes use of the Transport Management System (TMS) TMSX, creating an internal transport order: the driver and truck’s registration number are now present in TMSX.

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

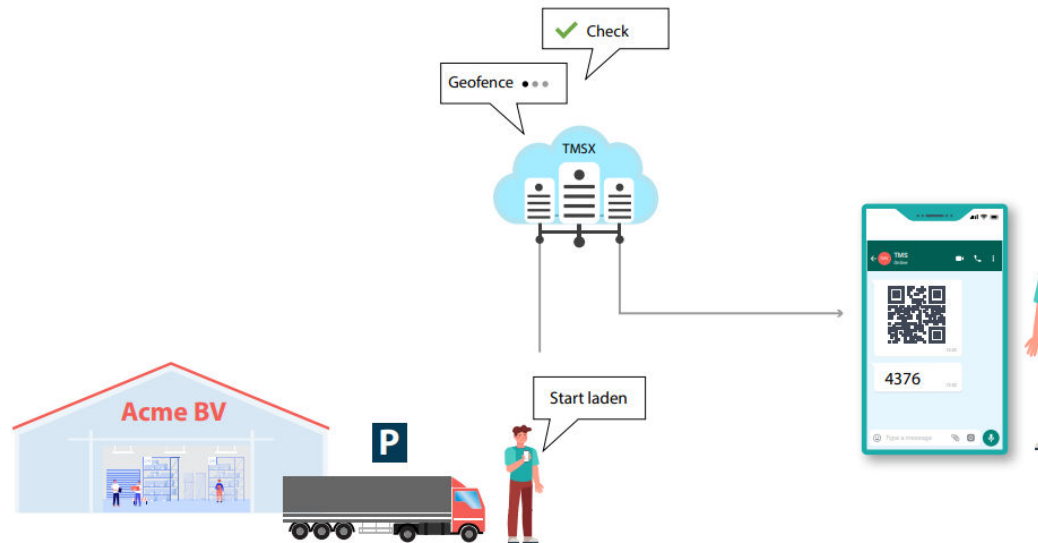


The digital proof of the transport order is present in TMSX

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



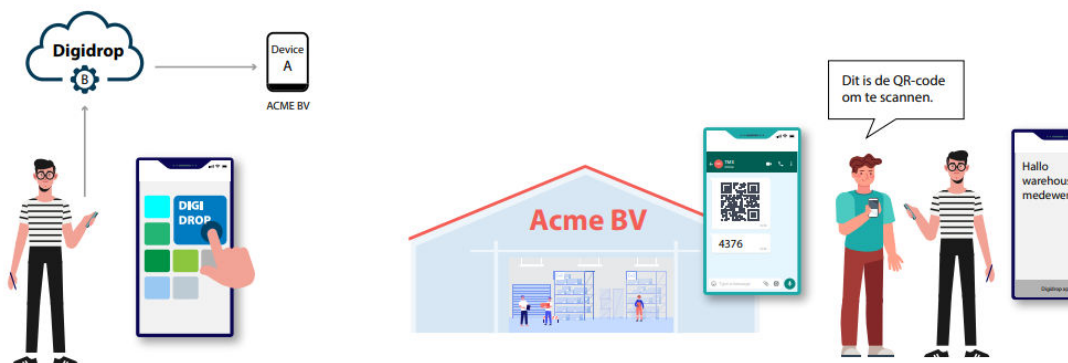
The driver takes the truck to the Acme BV warehouse, parks it, notifies TMSX that they will start loading and reports to the warehouse to collect the pallets.



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.

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.



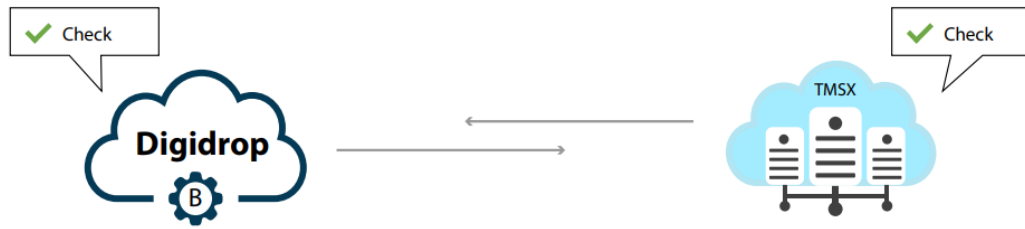
The warehouse employee scans the QR code using the app. The QR code contains:

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

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 JWT 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?



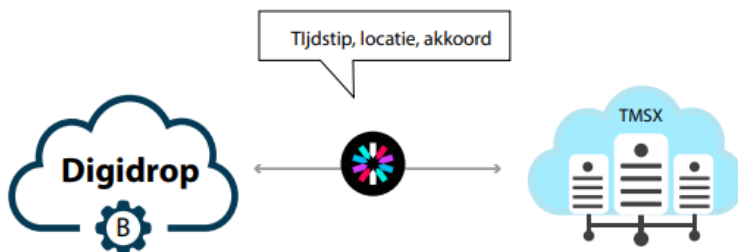
If this is all satisfactory, the warehouse employee will be asked to “enter the PIN”: this is the PIN the driver received via WhatsApp. The driver passes it on to the warehouse employee.²



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

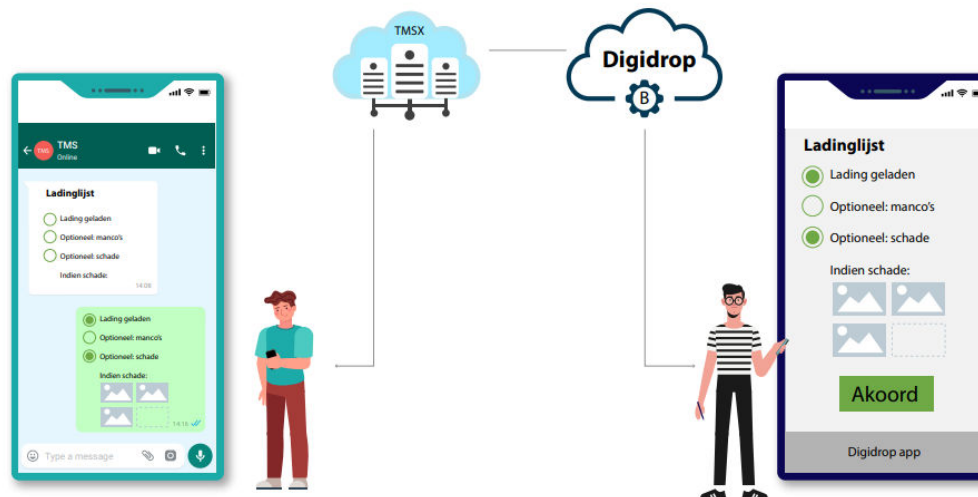
The warehouse employee confirms the details in the app, after which the cargo can be loaded.



² The PIN adds little in terms of proof, nor is it a GDPR relevant action, but it does create a barrier to showing data to the employee with an intended psychological effect.

The DigiDrop provider and TMSX exchange the digital proof of the confirmation (time, location, etc.)³

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.



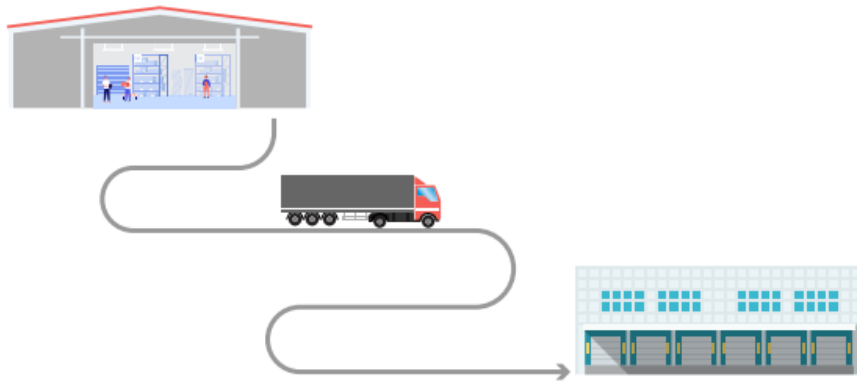
The DigiDrop providers sends TMSX signed digital proof of the approval.

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 DigiDrop signs a JWT, which is sent to TMSX.



3. Holder qualifications

The payload of the JWT 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 JWT (the liable organisation) has made this statement: the person that was sent has the necessary "papers".

4. Compliance

In this scenario, during a trip, an transportation inspector stops the truck and asks for details.

- The driver notifies TMSX that there is an inspection.
 - o TMSX verifies the geolocation of the phone and the truck: they must be in each other's vicinity
 - o 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:
 - o The inspector's device location/IP address
 - o The TMSX identity (digital)
 - Whether the party is known and certified
- The inspectorate's IT system identifies itself in TMSX and requests the JWT in question.
- The inspectorate's IT system assesses the JWT:
 - o Checking of order information and shipment
 - o Checking of transporter
 - o Checking of identity signing (TMSX)
 - o Checking of order issuing (who engaged the transporter)
 - o 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.

Analysis

Before delving into each scenario it should be emphasised that the humans involved do not act as legal agents of principals, able to legally bind said principals on their behalf, but as agents that are attributable to said entities in terms of factual acts on behalf of their principals. Scenario 1 is about the question under what circumstances a lorry driver is factually acting on behalf of a shipper, scenario 2 is about the recipient of a cargo being represented by humans at the unloading dock.

1. Attestation of representation: e.g. a lorry driver does represent a shipper that has been contracted to collect/deliver a load

In order to answer the core issue at hand, it is important to delve into the rules of evidence in Dutch private law. This is because the current (analogue) practice of considering a signed bill of lading as sufficient proof of the holder of that document to be authorised to haul a load of cargo, provided they can show a copy.

A general rule in the rules of evidence in private law is that it is up to the courts to accept statements and documents as evidence (or not). This means that it is possible that a court attaches more credibility to an oral statement than a written and signed document. Article 152 Rv can be translated as follows:

1. Evidence can be provided by any means, unless statute law stipulates otherwise.
2. Evaluation of evidence is left to the judgment of the judge, unless statute law stipulates otherwise.

A means of evidence can be an *akte* (not translated on purpose since this has a specific meaning in Dutch private law, but a close analog in English would be a deed), as defined in article 156 Rv, which can be translated as:

1. *Akten* are **signed documents**, intended as evidence.
2. *Authentieke akten*⁴ are *akten* in the required form and written down by officers⁵, who have been tasked by statute law to, through these means, reveal the observations made by them, or acts executed by them. As *Authentieke akten* are also considered those whose writing down is reserved to such officers, but whose writing down in specific cases has been tasked by statute law to others than officers.
3. *Onderhandse akten* are all *akten* that are not *authentieke akten*.

⁴ The closest analogues in common law are notarized deeds.

⁵ These are not necessarily civil servants, in practice these are notaries.

The subsequent question is how broadly the concept of “signed document” as meant in artikel 156 Rv should be read. Article 3:15a BW ties this into the eIDAS Regulation:

*As well as an **electronic advanced signature** as meant in article 3, section 12, of Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ 2014, L 257) have **advanced electronic signatures** as meant in section 11, and any other **electronic signatures** as meant in section 10, of article 3 of said regulation **the same legal effect as a handwritten signature**, provided that for each electronic signature the method of signing is sufficiently trustworthy, **considering the purposes for which the electronic signature has been used and all other circumstances of the case.***

The above quotation mentions the concepts electronic signature, advanced electronic signature and electronic qualified signature in the reverse order they are defined in article 3 eIDAS Regulation. For purposes of readability they are dealt with in the same order as in article 3 eIDAS Regulation.

Article 3 section 10 eIDAS Regulation provides the following definition:

“electronic signature” means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

An intermediate conclusion is that a JWT **potentially can function** as a electronic signature as meant in the eIDAS Regulation, depending on the purpose and all other circumstances of the application.

Article 3 section 11 provides the following definition:

“advanced electronic signature” means an electronic signature which meets the requirements set out in Article 26;

Said requirements in article 26 are as follows:

An advanced electronic signature shall meet the following requirements:

- a) it is uniquely linked to the signatory;*
- b) it is capable of identifying the signatory;*
- c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and*
- d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.*

When applying the aforementioned requirements to the JWT as envisaged in the BDI:

- a) uniquely linked to the signatory: appendix 2 to the BDI documentation⁶ describes a register of representatives, without describing how to safeguard the correctness of such a register. In light of the jurisprudence, especially ECLI:NL:RBROT:2022:3242 and ECLI:NL:RBROT:2023:10194 it should be mentioned that this linkage is not yet sufficiently provided for. It should also be mentioned that this is not inherent to the JWT technology, but on how its application is organised;
- b) capable of identifying the signatory: the arrangements chosen in the BDI documentation explicitly allow for this, partly through the registration of personal data of agents signing on behalf of the actual signatories (to which there is a separate GDPR-dimension since regardless of their quality as agents for other actors, this still involves personal data);
- c) created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control: a similar conclusion as under a), the BDI documentation does not provide for such a high level of confidence, but this again is a matter of implementation and not so much of the JWT technology;
- d) linked to the data signed therewith in such a way that any subsequent change in the data is detectable: the choices made, including asymmetric cryptography, allow for this criterium to be met.

A further intermediate conclusion is that a JWT in the context of BDI potentially qualifies as an advanced electronic signature as meant by the eIDAS Regulation, but that the current state of the BDI documentation does not yet contain the choices necessary for fulfilling this potential.

For the sake of completeness it is also worth to briefly touch upon qualified electronic signatures, which are defined in article 3 section 12 eIDAS Regulation as:

*“qualified electronic signature” means an **advanced electronic signature** that is created by a **qualified electronic signature creation device**, and which is based on a **qualified certificate** for electronic signatures;*

The qualified certificate and the qualified electronic signature creation device (in practice a certified hardware security module) require the involvement of a trust service provider. Annex I to the eIDAS Regulation describes the criteria for qualified certificates that are used by a qualified electronic signature creation device. These requirements are mostly legal and organisational and do not preclude a JWT to satisfy these requirements. Since article 3:15a BW do not require a qualified electronic signature for equivalence to a handwritten signature, further analysis is not needed for now.

2. transfer of cargo: proof of receipt or release of the possession of a load

Applying the earlier analysis and the rules of evidence in Dutch law to this scenario, a major difference stand out:

⁶ See footnote 1.

- The chain of evidence relies heavily on data in the TMS. So the JWTs should not be considered as documentation signed by the actors described in this scenario, but as documentation signed by whoever controls the TMS.
- In that sense the TMS operator becomes a third party making claims about events that can still become evidence in for example a court case about a disappearance of a cargo.
- In the eIDAS 2.0 Regulation there are several trust providers introduced that map to some extent to what the TMS operator does in this use case. The one that maps the closest seems to be that of the electronic ledger defined in article 1, section 52 of the eIDAS 2.0 Regulation:

“electronic ledger” means a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records

Very little about these electronic ledger services is actually regulated by the eIDAS 2.0 regulation in articles 45k (legal effects of electronic ledgers) and 45l (requirements for qualified electronic ledgers).

The proposed DigiDrop solution could qualify as an electronic ledger, provided that the events recorded are in such a way that the integrity of the recording and the accuracy of chronological ordering are safeguarded.

Applying article 45k eIDAS 2.0 to it, which says:

1. *An electronic ledger shall not be denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers.*
2. *Data records contained in a qualified electronic ledger shall enjoy the presumption of their unique and accurate sequential chronological ordering and of their integrity.*

Means that the DigiDrop-concept at least cannot be denied admittance in court proceedings, but then under Dutch rules of evidence in private law this would be the case anyway.

For this to be strengthened to a level comparable to that of for example qualified electronic signatures, this would need to meet the criteria of article 45l eIDAS 2.0 Regulation. However, at this time it is yet unclear what these criteria actually are since the technical details are delegated to delegated acts by the European Commission through the so-called comitology-procedure.

However, another way to potentially strengthen the already existing evidence power of this application of JWTs would be to combine the DigiDrop solution with terms and conditions in the relevant transport agreements. In Dutch law there is room for so-called

“bewijsovereenkomsten” (evidence agreements). This concept is ruled by article 153 Rv which (roughly translated) says:

Agreements deviating from the statutory rules of evidence shall not apply if they relate to the proof of facts to which the law attaches consequences which are not at discretion of the contracting parties, without prejudice to the grounds on which they remain inapplicable under the Civil Code.

The give an example of an agreement that would constitute an inapplicable deviation would be if contracting parties were agree that despite statutory law requiring a notarised deed for the sale of real estate, the parties accepting a normal contract. The opposite however, if contracting parties agree that between them a log of events at a third party, e.g. a TMS provider, can be used as evidence, and there is no statutory law to the contrary, is possible under Dutch law. Similarly, the contracting parties can agree additional authentication instruments for notifying each other of relevant events or to authenticate (sign) documents. The most commonly used version of this prior to 2009 used to be the parts of banking terms and conditions that regulate the use of a PIN authenticating for electronic bank transfer and withdrawals, which have been partially superseded by a relevant section in the Dutch civil code governing payment services. A very early case regarding this, is aforementioned ECLI:NL:HR:1993:ZC1148, in which the dispute was about a bank transfer that had been initiated via an encrypted telex message. Since the initiating party of said transfer had indemnified the bank for any unauthorised bank transfers accompanied by the correct codes, these codes de facto performed the role of a digital signature authenticating the payment order.

In conclusion, while the DigiDrop solution may in the future meet eIDAS 2.0 requirements for being an electronic ledger providing evidence of events that are relevant for the start or fulfilments of obligations in logistics, it currently cannot do so for lack of flanking terms and conditions.

Such flanking terms and conditions can, given the experience in banking law, change the rules of evidence in a way that is within the discretion of the partner. It therefore would be advisable to create such flanking terms and conditions.