

# JSON Web Signature (JWS) als generiek digitaal bewijs tussen organisaties



# Colofon

---

## JSON Web Signature (JWS) als generiek digitaal bewijs tussen organisaties

### Auteurs

H. Wagter

S. Schouten

Januari 2025

© Connekt



# Samenvatting

---

Er is een toenemende behoefte zichtbaar in zakelijk verkeer om bewijsvoering bij interacties tussen bedrijven onderling, en tussen bedrijven en toezichthouders te digitaliseren. Het gaat om:

- **Bewijs van vertegenwoordiging (persoon namens organisatie)**
- **Overdracht van lading tussen partijen**
  - Ophalen van een zending;
  - Lossen van een zending.
- **Bewijs van kwalificaties (van persoon namens organisatie)**
- **Bewijs van voldoen aan regels en wetten**

De mensen of systemen die ingeschakeld worden om het werk te doen handelen namens de bedrijven of toezichthouders: het zijn de organisaties die aansprakelijk zijn, niet de mensen (uitzonderingen daargelaten). Het zou nuttig zijn als er een manier is waarbij:

- Er een (juridisch en praktisch) sterk digitaal bewijs geleverd wordt van de ene partij aan de andere, in plaats van een papieren bewijs.
- Er een werkproces is wat past bij de (diverse) praktijk, met wisselend en soms tijdelijk personeel dat weinig (IT-)opleiding heeft, en beperkte kennis van systemen en processen heeft.
- De oplossing breed toe te passen is tegen acceptabele kosten.
- Er een vrije markt voor IT-dienstverleners ontstaat die deze oplossingen kunnen aanbieden in concurrentie.

Dit document beschrijft een generiek inzetbare methode die aan deze voorwaarden voldoet.<sup>1</sup>

Na 2010 is een nieuwe standaard<sup>2</sup> voor digitale bewijzen populair geworden (JSON Web Token, of JWT). De momenteel meest gebruikte toepassing van getekende JWT's is als bewijs tussen IT-systemen, tussen servers: het is een beproefde manier om rechten en identiteiten van gebruikers te delen, welbekend en met veel ondersteuning.

Een getekende JWT voldoet aan de JSON Web Signature (JWS)<sup>3</sup> specificatie: een JWS is de algemene standaard om inhoud (een document bijvoorbeeld) met zekerheid over te dragen, een JWT is specifiek gericht op 'claims', de vraag van vertrouwen in identiteiten.

---

<sup>1</sup> Verifiable Credentials en wallets zijn een mogelijk alternatief dat in de toekomst breed geaccepteerd zou kunnen gaan worden. Een JWT is een formaat wat daarmee compatibel is.

<sup>2</sup> Zie bijlage 2.

<sup>3</sup> [RFC 7515 - JSON Web Signature \(JWS\)](#)

---

Het digitale bewijs in een JWS bestaat uit drie samenhangende delen:

- **De inhoud**
  - datgene wat beweerd wordt door de zender;
  - met eventueel additionele gegevens zoals een geldigheidsduur.
- **Het bewijs dat de inhoud niet gewijzigd is sinds het moment van versturen door de zender**
  - hash of fingerprint.
- **Het bewijs dat de inhoud plus het bewijs van 'niet gewijzigd' echt verstuurd is door de zende partij, en niet door een ander met een valse identiteit**
  - tekenen (cryptografische bewerking) met een erkend certificaat dat bij de afzender hoort.

Voor belangrijke gegevens die veel waarde vertegenwoordigen kunnen certificaten van hoge kwaliteit toegepast worden. Neem bijvoorbeeld de EIDAS certificaten ('sealed digital documents'). Bij toepassing van die certificaten voldoet het 'tekenen' aan de hoogste eisen van elektronische handtekeningen<sup>4</sup>.

De standaard staat toe dat JWS's in elkaar verpakt worden. Dat wil zeggen dat de inhoud van een JWS weer een andere JWS kan zijn, net als een envelop binnen een envelop. Die eigenschap is zeer praktisch in logistieke toepassingen: het bewijs dat een bedrijf namens een opdrachtgever optreedt wordt zo in één keer geleverd. Er is op zich geen formele limiet aan het aantal keren dat er 'embedded' kan worden maar de uiteindelijke JWS wordt steeds groter in aantal kilobytes<sup>5</sup>.

Voor veel toepassingen is gebruikersgemak belangrijker dan hoge zekerheden inbouwen. Voor dat soort situaties is een vorm uitgewerkt die is geïnspireerd door het gebruikersgemak van DigiD en 'Tikkie'.

Net zoals bij DigiD hebben gebruikers in deze variant niet veel meer nodig dan een smartphone, QR-codes en pincodes. Het ingewikkelde deel van de uitwisseling gaat met professionele techniek tussen IT-systemen van twee partijen.

De grote denkstap in deze opzet is dat IT-systemen namens hun bedrijven 'electronische handtekeningen' uitwisselen. Ze zijn gemandateerd (op digitale wijze) om dat te doen. De mensen in dit scenario zetten geen 'handtekeningen'. Ze zijn inwisselbare 'operators' die een stukje bewijsvoering toevoegen aan het totaal aan bewijzen dat de overdracht gaat zoals verwacht.

---

<sup>4</sup> [https://www.etsi.org/deliver/etsi\\_ts/119100\\_119199/11918201/01.02.01\\_60/ts\\_11918201v010201p.pdf](https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.02.01_60/ts_11918201v010201p.pdf)

<sup>5</sup> Deze grote JWS's kunnen niet meer via een HTTP-request (header) worden doorgegeven, maar worden in de body van een request geplaatst.

---

Dat totaal aan bewijzen bestaat uit bijvoorbeeld:

- Het tijdstip.
- De locatie.
- Het kenteken van de vrachtwagen, de naam van de transporteur, het ID-bewijs van de chauffeur
- De identificatie van de zending.
- Het apparaat wat de magazijnmedewerker gebruikt, met additionele kenmerken zoals IP-adres, Mac-adres of andere kenmerken.
- De waarschijnlijkheid dat de magazijn medewerker en de chauffeur op hetzelfde moment op dezelfde plek zijn en elkaar zien.
- Foto van de lading.

Dat totaal aan bewijzen kan voldoende zijn voor de betrokken bedrijven om een overdracht te laten 'ondertekenen' door hun IT-systemen. De oplossing is flexibel: zowel qua inhoud als met de mogelijkheid om last-minute wijzigingen door te voeren. De juridische sterkte is hoog, indien de implementatie professioneel gedaan wordt.

De oplossing is breed toepasbaar, ook bij interacties met de overheid: een voorbeeld van het laatste is het managen van privileges om lege vrachtwagens over een zwakke brug te laten rijden.

Het BDI afsprakenstelsel ondersteunt deze werkwijze op meerdere manieren:

- met extra vertrouwen in partijen ('certificering');
- met gedeelde algemene voorwaarden die specifiek geschreven zijn voor deze toepassing;
- met laagdrempelige hybride varianten om partijen met weinig IT-mogelijkheden toch operationeel te integreren ('Edge Agreements').

# Inhoud

---

<b>1.</b>	<b>De behoefte aan digitaal bewijs tussen organisaties</b>	<b>7</b>
<b>2.</b>	<b>Digitaal bewijs</b>	<b>8</b>
2.1	Identiteitsbewijs en certificaten apart	9
2.2	Bewijs in een bewijs: nuttig bij uitbesteding	9
2.3	Flexibel: last-minute aanpassingen	9
<b>3.</b>	<b>Toepassen in de praktijk: bedrijven onderling</b>	<b>11</b>
3.1	DigiDrop basis	13
3.2	Obstakels	17
	Geen mobiel internet in magazijn	17
	De magazijnmedewerker kan geen QR-code scannen	17
	Het apparaat van de magazijnmedewerker is kapot of heeft geen verbinding	17
	TMSX is tijdelijk niet beschikbaar	17
3.3	Een magazijn heeft geen DigiDrop Provider	17
3.4	Opnemen in algemene voorwaarden	18
<b>4.</b>	<b>Werkwijze bij aantonen professionele diploma's en certificaten</b>	<b>19</b>
<b>5.</b>	<b>Toepassen in de praktijk voor toezichthouders</b>	<b>20</b>
5.1	Open 4 corner model voor inspecties	20
5.2	Bewijs leveren aan de inspecteur	21
5.3	Breder gebruik: privileges	24
<b>6.</b>	<b>Marktwerving</b>	<b>26</b>
<b>7.</b>	<b>Ondersteuning door het BDI-stelsel</b>	<b>27</b>
7.1	Vertrouwen in partijen	27
7.2	Gedeelde algemene voorwaarden	27
7.3	Gedeelde semantiek	27
7.4	Gedeelde services	27
<b>8.</b>	<b>Hybride werkmethodes</b>	<b>28</b>
8.1	Edge Agreement DigiDrop UltraLite	28
8.2	Edge Agreement DigiDrop Lite	30
	<b>Bijlage 1: JWS en QR-codes</b>	<b>31</b>
	<b>Bijlage 2 : Relevante IT standaarden</b>	<b>32</b>

# 1 De behoefte aan digitaal bewijs tussen organisaties

---

In zakelijk verkeer (handel en dienstverlening) zijn er regelmatig momenten waarbij er een bewijs geleverd moet worden tussen organisaties: tussen bedrijven onderling, en naar toezichthouders. In de huidige praktijk spelen mensen en (papieren) documenten daarbij een grote rol.

Als we ons richten op logistiek/transport en dienstverlening/service zijn de meest voorkomende situaties:

## **Bewijs van vertegenwoordiging**

- Komt de persoon die voor ons staat namens de originele opdrachtgever, en voor de specifieke opdracht? En kunnen we het bedrijf waarvoor deze persoon werkt daarvoor aansprakelijk stellen?

## **Overdracht van lading tussen partijen**

- Ophalen van een zending.
- Lossen van een zending.

## **Bewijs van kwalificaties**

- Heeft de persoon die voor ons staat inderdaad de juiste diploma's, trainingen of certificaten, en kunnen we het bedrijf waarvoor deze persoon werkt daarvoor aansprakelijk stellen?

## **Bewijs van voldoen aan regels en wetten**

- Kan de toezichthouder of controleur verifiëren of alles volgens de regels wordt uitgevoerd (compliance)? Zowel bij inspectie onderweg als aan de hand van ingediende documenten?

De mensen of systemen die ingeschakeld worden om het werk te doen handelen namens de bedrijven of toezichthouders: het zijn de organisaties die aansprakelijk zijn, niet de mensen (uitzonderingen daargelaten).

In veel gevallen is er daarbij ook nog sprake van uitbesteding van werk: het kan zo zijn dat een transportorder een paar keer onder-uitbesteed wordt. De chauffeur die lading komt ophalen kan een zelfstandige zijn die tijdelijk werkt voor een kleine transporteur, die op zijn beurt ingeschakeld wordt door een grote logistieke dienstverlener die namens de ladingeigenaar de opdracht uitvoert. Een servicemonteur kan een zelfstandige zijn die ingeschakeld wordt door een klein servicebedrijf wat door een groot servicebedrijf ingehuurd wordt om onderhoud te doen voor een fabrikant van apparatuur.

Er is een toenemende behoefte zichtbaar om die bewijsvoering te digitaliseren.

Het zou nuttig zijn als er een manier is waarbij:

- Er een (juridisch en praktisch) sterk digitaal bewijs geleverd wordt van de ene partij aan de andere, in plaats van een papieren bewijs.
- Er een werkproces is wat past bij de (diverse) praktijk, met wisselend en soms tijdelijk personeel dat weinig (IT-)opleiding heeft, en beperkte kennis van systemen en processen heeft.
- De oplossing breed toe te passen is tegen acceptabele kosten.
- Er een vrije markt voor IT-dienstverleners ontstaat die deze oplossingen kunnen aanbieden in concurrentie.

Dit document beschrijft een generiek inzetbare methode die aan deze voorwaarden voldoet.

## 2 Digitaal bewijs

Na 2010 is een nieuwe standaard voor digitale bewijzen populair geworden (JSON Web Token, of JWT)<sup>6</sup>. De momenteel meest gebruikte toepassing van getekende JWT's is als bewijs tussen IT-systemen, tussen servers: het is een beproefde manier om rechten en identiteiten te delen van gebruikers. De open standaard OAuth baseert zich bijvoorbeeld op deze technologie. Het brede gebruik betekent dat er ondersteuning zoals softwarebibliotheken beschikbaar is in diverse programmeertalen.

De standaard is flexibel en staat meer toe dan nu gangbaar is<sup>7</sup>.

Een getekende JWT voldoet aan de JSON Web Signature (JWS) specificatie: een JWS is de algemene standaard om inhoud (een document bijvoorbeeld) met zekerheid over te dragen, een JWT is specifiek gericht op 'claims', de vraag van vertrouwen in identiteiten.

**JWT:** Is een toepassing van JWS die specifiek wordt gebruikt voor het overdragen van **claims**. Dit zijn stukjes informatie (zoals een gebruikers-ID, toegangsrechten of sessiedetails) die gebruikt worden in systemen voor authenticatie en autorisatie. JWT's worden bijvoorbeeld veel gebruikt in Single Sign-On (SSO) oplossingen en API-toegang.

**JWS:** Is ontworpen om **algemene gegevens** te beveiligen door een digitale handtekening toe te voegen, waarmee de integriteit van de gegevens en de authenticiteit van de afzender gewaarborgd kunnen worden. Het wordt breed toegepast in situaties waar veilige gegevensoverdracht belangrijk is.

Dit document past de JSON Web Signature (JWS) Unencoded Payload Option<sup>8</sup> toe omdat deze standaard beter geschikt is voor embedding dan andere JWS standaarden<sup>9</sup>.

Het digitale bewijs in een JWS bestaat uit drie samenhangende delen:

- **De inhoud**
  - datgene wat beweerd wordt door de zender, de gegevens waar het om gaat;
  - met eventueel additionele gegevens zoals een geldigheidsduur.
- **Het bewijs dat de inhoud niet gewijzigd is, sinds het moment van versturen door de zender**
  - hash of fingerprint<sup>9A</sup>.
- **Het bewijs dat de inhoud plus het bewijs van 'niet gewijzigd' echt verstuurd is door de zendende partij, en niet door een ander met een valse identiteit**
  - tekenen (cryptografische bewerking) met een erkend certificaat dat bij de afzender hoort.

De wiskundige basis (cryptografie) voor die bewijzen is algemeen bekend en wordt op vrijwel het gehele Internet gebruikt voor belangrijke transacties. Dit soort bewijzen zijn juridisch sterk indien de implementatie goed uitgevoerd is. Goed uitvoeren betekent onder andere de juiste variant in de standaard kiezen, e.e.a. organisatorisch goed inrichten en de juiste certificaten gebruiken.

<sup>6</sup> [RFC 7519: JSON Web Token \(JWT\)](#)

<sup>7</sup> *Verifiable Credentials en wallets zijn een mogelijk alternatief dat in de toekomst breed geaccepteerd zou kunnen gaan worden. Een JWS is een compatibel formaat.*

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

<sup>9</sup> <https://datatracker.ietf.org/doc/html/rfc7515> - JSON Web Signature (JWS), zie bijlage 2.

<sup>9A</sup> [SHA-2 - Wikipedia](#)

Voor belangrijke gegevens<sup>10</sup> die veel waarde vertegenwoordigen kunnen certificaten van hoge kwaliteit toegepast worden. Neem bijvoorbeeld de EIDAS certificaten ('seals'). Bij toepassing van die certificaten voldoet het 'tekenen' aan de hoogste eisen van elektronische handtekeningen<sup>11</sup>.

Het digitale bewijs kan voor onbeperkte tijd opgeslagen worden, de 3-eenheid (inhoud, bewijs inhoud is onveranderd, bewijs wie het verstuurd heeft) is altijd van kracht. Als iemand achteraf de inhoud zou aanpassen is dat direct zichtbaar.

Er zijn een aantal standaard 'inhoud' definities, maar verder staat het iedereen vrij om eigen inhoud te definiëren. Dat biedt veel mogelijkheden.

Een digitaal bewijs bij transport kan bijvoorbeeld als inhoud hebben:

- Het kenteken van de vrachtwagen.
- Naam en ID-nummer van de chauffeur.
  - Eventueel speciale certificaten van de chauffeur, zoals gevaarlijke goederen of veiligheidstrainingen.
- Gegevens van de lading, adressen etc.
- De digitale identiteit van de transporteur en van de opdrachtgever.
- Het bewijs dat de opdrachtgever de transportopdracht gegeven heeft aan deze transporteur.
- Tijdstip en locatie van de overdracht.
- Additionele documenten
- Foto's
- Enz.

## 2.1 Identiteitsbewijs en certificaten apart

Het is goed om op te merken dat dit digitale bewijs in de basis geen vervanger is van een identiteitsbewijs. Het idee is dat een persoon een apart identiteitsbewijs of ID-kaart heeft. De inhoud van de JWS dient om te bewijzen dat de opdrachtgever iemand stuurt met een bepaalde naam en identiteitsbewijs. Een bewaker kan het ID-bewijs controleren en vergelijken met de inhoud van de JWS: als die matchen kan de persoon verder.

De standaard voor een JWS staat echter wel toe dat moderne digitale certificaten van identiteit en diploma's (verifiable credentials/verifiable presentations) meegestuurd worden in de JWS. De methode is daarmee toekomstvast.

## 2.2 Bewijs in een bewijs: nuttig bij uitbesteding

De standaard staat toe dat een complete JWS als digitaal bewijs 'ingepakt' wordt als deel van de 'inhoud' in een ander digitaal bewijs (JWS): een envelop binnen een envelop als het ware. In principe is er geen limiet aan het 'in elkaar inpakken'.

<sup>10</sup> Zoals belangrijke vrachtbrieven, Bill-of-Lading

<sup>11</sup> De EIDAS standaard voor het toevoegen van elektronische handtekeningen in JWT's of JWS is hierbij relevant: [https://www.etsi.org/deliver/etsi\\_ts/119100\\_119199/11918201/01.02.01\\_60/ts\\_11918201v010201p.pdf](https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.02.01_60/ts_11918201v010201p.pdf)

---

Het in elkaar verpakken van bewijzen is heel nuttig bij uitbesteding.

Neem een transportopdracht:

- Het eerste digitale bewijs (JWS) kan de transportopdracht zijn: deze transporteur is inderdaad door de verkoper ingeschakeld om deze lading te transporteren.
- De eerste JWS zit weer verpakt in de volgende JWS: het digitale bewijs dat deze chauffeur en truck/kenteken opdracht gekregen om namens de transporteur het werk te doen.

Met één digitaal bewijs kan zo de keten van opdrachtverlening bewezen worden<sup>12</sup>.

Hetzelfde werkt bij dienstverlening: de keten van opdrachtverlening is bij elkaar verpakt. Het is vrij eenvoudig om te specificeren dat in elke JWS een link zit naar de maker van de JWS. Door de link te volgen is realtime te verifiëren dat de maker van de JWS nog steeds bevestigt dat de JWS en dus het bewijs geldig is. Door dat achter elkaar voor elke 'in elkaar verpakte' JWS te doen wordt de keten geverifieerd.

### **2.3 Flexibel: last minute aanpassingen**

Het aanmaken van een JWS kost relatief weinig tijd en rekenkracht. Die eigenschappen maken het makkelijk om last-minute wijzigingen door te voeren bij het aanmaken van de JWS.

Bijvoorbeeld: als er toch een ander kenteken met een andere chauffeur gestuurd wordt dan eerst bedacht was. Dan is een nieuwe inhoud in een JWS stoppen zo gebeurd.

---

<sup>12</sup> Technisch zijn er twee type oplossingen: de hele getekende JWS opnemen in een andere, of alleen een link naar de bron van de JWS opnemen. Elk heeft zijn voor- en nadelen. In deze beschrijving is uitgegaan van het geheel opnemen van een JWS in de 'envelop' van een andere JWS, als meest robuuste manier.

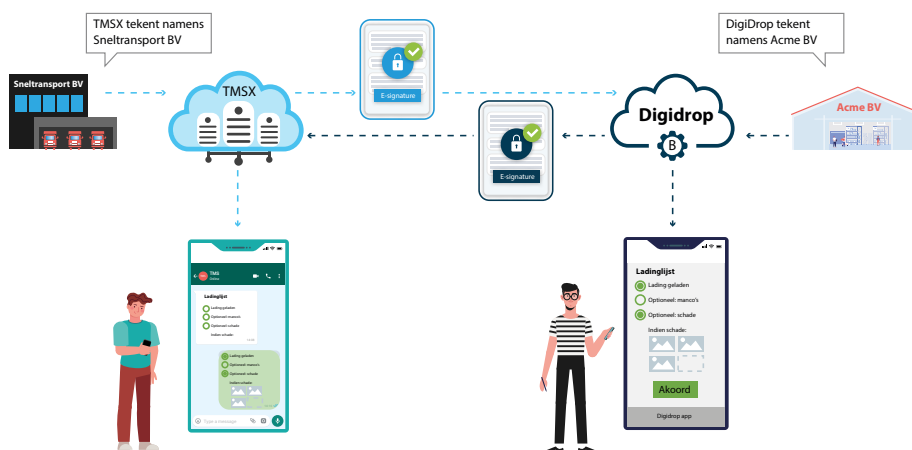
### 3 Toepassen in de praktijk: bedrijven onderling

Alhoewel dit soort digitale bewijzen in de IT breed bekend zijn vraagt deze technologie een behoorlijke technische kennis en de nodige professionaliteit van implementatie en beheer. Zo is kennis van digitale certificaten nodig en het kunnen omgaan met grote digitale bewijzen.

Hoe kun je ze dan toch simpel en makkelijk toepasbaar maken in de logistiek, voor mensen met nauwelijks IT-opleiding?

De inspiratie is te vinden bij DigiD en bij de welbekende 'Tikkie'. Makkelijk om toe te passen, de moeilijke techniek regelen professionele bedrijven op de achtergrond. De mensen gebruiken bekende hulpmiddelen (app, chat, mail, QR-codes, links, pincode) om keten te sluiten.

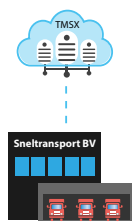
De grote denkstap in deze opzet is dat IT-systemen namens hun bedrijven 'electronische handtekeningen' uitwisselen. Ze zijn gemandateerd (op digitale wijze) om dat te doen.



*Elektronische handtekeningen tussen DigiDrop en TMSX namens de opdrachtgevers*

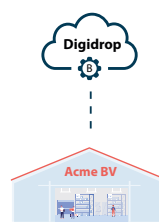
De mensen in dit scenario zetten geen 'handtekeningen'. Ze zijn inwisselbare 'operators' die een stukje bewijsvoering toevoegen aan het totaal aan bewijzen dat de overdracht gaat zoals verwacht. Dat totaal aan bewijzen bestaat uit bijvoorbeeld:

- Het tijdstip.
- De locatie.
- Het kenteken van de vrachtwagen, de naam van de transporteur, het ID-bewijs van de chauffeur
- De identificatie van de zending.
- Het apparaat wat de magazijnmedewerker gebruikt, met additionele kenmerken zoals IP-adres, Mac-adres of andere kenmerken.
- De waarschijnlijkheid dat de magazijnmedewerker en de chauffeur op hetzelfde moment op dezelfde plek zijn en elkaar zien.
- Foto van de lading.



**Zekerheid**  
voor TMSX en Sneltransport BV

- Identiteit Digidrop partij
- Geolocatie devices en tijdstip
- Orderinformatie
- Chauffeur heeft magazijnmedewerker ontmoet die gegevenscheck heeft gedaan
- Chauffeur bevestigt transfer
- Eventueel fotos en tekst
- Bevestiging door Digidrop
- E-handtekening door Digidrop



**Zekerheid**  
Zekerheid voor Digidrop en Acme BV

- Identiteit TMSX partij
- Geolocatie devices en tijdstip
- Orderinformatie
- Magazijn medewerker heeft chauffeur ontmoet en gegevenscheck gedaan
- Magazijnmedewerker bevestigt transfer
- Eventueel fotos en tekst
- Bevestiging door TMSX
- E-handtekening door TMSX

Dat totaal aan bewijzen kan voldoende zijn voor de betrokken bedrijven om een overdracht te laten 'ondertekenen' door hun IT-systemen. De onderling afgesproken voorwaarden leggen daarvoor de juridische basis.

Deze aanpak zorgt ervoor de IT-systemen van bedrijven een digitale handtekeningen kunnen zetten, gebaseerd op een combinatie van verzamelde bewijzen. Menselijke betrokkenheid beperkt zich tot een operationele rol waarin zij gegevens vastleggen, maar de daadwerkelijke 'ondertekening' en validatie worden uitgevoerd door geautomatiseerde systemen. Dit systeem bouwt vertrouwen op door:

- **Contextuele data:**  
Tijdstippen, locaties, en identificatiegegevens van objecten, apparaten en personen.
- **Digitale integriteit:**  
Technieken zoals cryptografische handtekeningen waarborgen dat de gegevens authentiek en ongewijzigd blijven.

Dit proces maakt overdrachten juridisch afdwingbaar door de onderlinge afspraken tussen partijen en laat zien hoe technologie traditionele menselijke handelingen kan vervangen door betrouwbare, schaalbare digitale oplossingen.

De hieropvolgende beschrijving laat op versimpelde wijze de transport variant zien (in dit document met de naam 'DigiDrop' aangeduid). Deze opzet is bedacht voor de overdracht van goederen in de praktijk van wegtransport<sup>13</sup>.

De variant in de beschrijving probeert de eisen aan de apparatuur op de vloer zo laag mogelijk te houden. En rekening te houden met de obstakels in de praktijk (geen verbinding in het magazijn bijvoorbeeld) en terugvalopties<sup>14</sup>.

Het aantonen onder uitbesteding, aantonen professionele diploma's en certificaten, aantonen aan toezichthouders werkt functioneel vrijwel identiek.

De beschrijving in dit hoofdstuk is gericht op zakelijke interacties, de beschrijving voor gebruik door toezichthouders is er uitgelicht en in hoofdstuk 5 weergegeven.

<sup>13</sup> Voor de eenvoud van de uitleg zijn is één van de technische varianten gekozen die mogelijk zijn. In de nadere uitwerking zijn afwegingen te maken die de ene variant een voorkeur geven boven een andere.

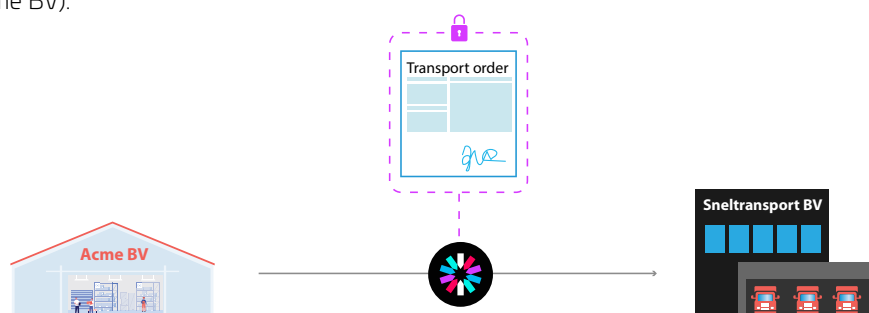
<sup>14</sup> In bijlage 1 wordt ingegaan op een aantal overwegingen.

### 3.1 DigiDrop basis

Eerst wordt de basisvariant uitgelegd, en daarna wat de terugvalopties zijn als er een obstakel is, bijvoorbeeld geen mobiel internet binnen het magazijn.

De uitleg gaat aan de hand van het voorbeeld van ophalen van goederen bij een magazijn. Het afleveren gaat op dezelfde manier, maar dan met een ontvangstmedewerker en de ontvanger.

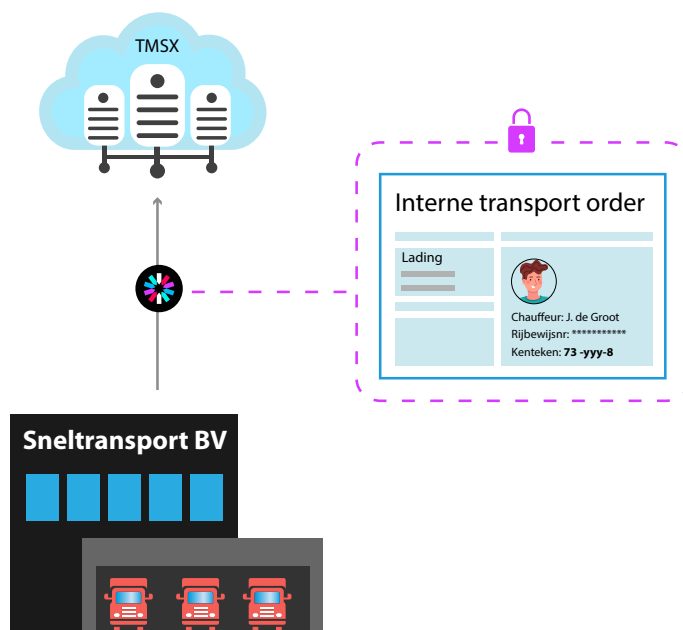
Een handelsmaatschappij (Acme BV) heeft een paar pallets met goederen verkocht en geeft een digitale transportorder aan Sneltransport BV. Dat gaat ook in de vorm van een digitaal bewijs (JWS, getekend door Acme BV).



*Acme BV stuurt een digitaal bewijs aan Sneltransport BV van de transportorder*

Sneltransport BV maakt gebruik van het Transport Management Systeem (TMS) TMSX, en maakt daarin een interne transportopdracht aan: chauffeur en kenteken van de vrachtwagen zijn nu bekend bij TMSX.

Sneltransport BV heeft bij het begin van de relatie TMSX een digitaal bewijs gegeven, dat aantoont dat TMSX namens Sneltransport mag optreden.

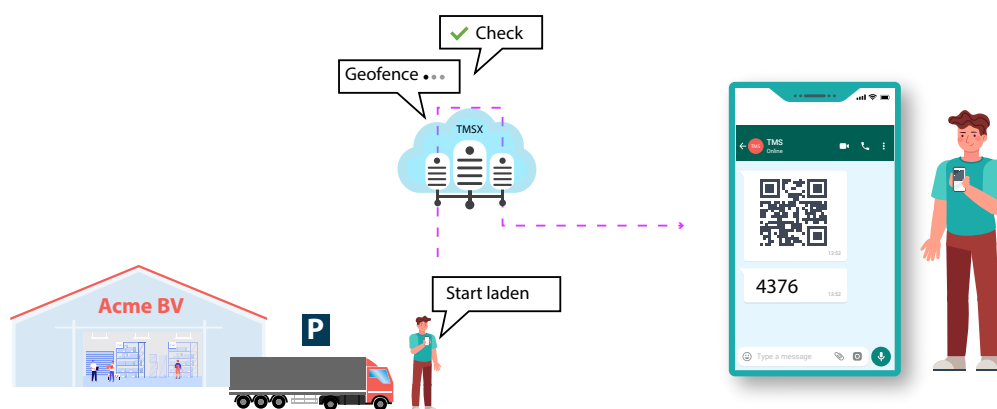


*Het digitale bewijs van de transportorder is bekend bij TMSX*

De chauffeur heeft een mobiele telefoon met Whatsapp: het nummer en de identiteit van de chauffeur (inclusief ID-nummer) zijn bekend bij TMSX.



De chauffeur gaat naar het magazijn van Acme BV toe, parkeert de vrachtwagen, meldt aan TMSX dat hij gaat laden en meldt zich aan bij het magazijn voor het ophalen van de pallets.



TMSX verifieert de geolocatie van de telefoon en de vrachtwagen: dat moet in de buurt van het bekende adres zijn. TMSX stuurt een tijdelijke QR-code en een tijdelijke pincode via Whatsapp naar de chauffeur<sup>15</sup>

De magazijnmedewerker van Acme BV heeft een geregistreerde telefoon of een bedrijfstablet. Die is geregistreerd bij de DigiDrop provider van Acme BV (een nieuwe rol) als in bezit van Acme BV. Op de telefoon staat de app van de DigiDrop provider.



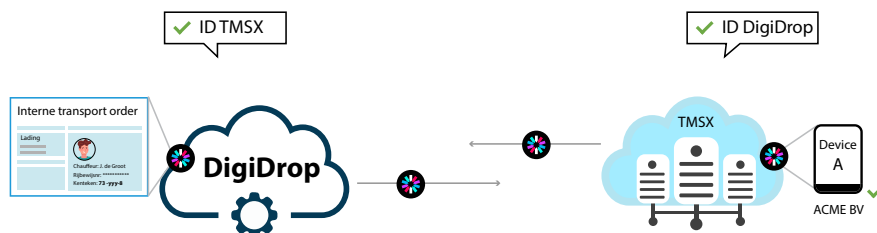
De magazijnmedewerker scant de QR-code met de app. De QR-code bevat:

- Een link naar de DigiDrop server van TMSX.
- Een unieke tijdelijke code voor deze overdracht.

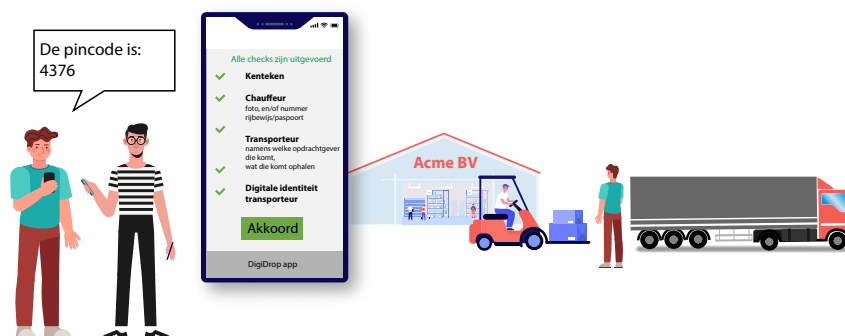
<sup>15</sup> Voor de duidelijkheid van de uitleg zijn pincode en QR-code in 1 plaatje samengevat. In de praktijk zullen die gescheiden aangeleverd worden.

De DigiDrop provider van Acme en TMSX gaan vervolgens het technologisch ingewikkelde werk doen van:

- Elkaars digitale identiteit verifiëren.
- Digitale bewijzen uitwisselen van vertegenwoordiging (TMSX namens Sneltransport. DigiDrop provider namens Acme BV).
- TMSX stuurt de JWS naar DigiDrop en die verifieert het bewijs: getekend? onveranderd?
- Inhoud uitpakken en bekijken, en verifiëren tegen andere informatie.
  - Kloppen de gegevens met locatie, identiteiten en interne orders?



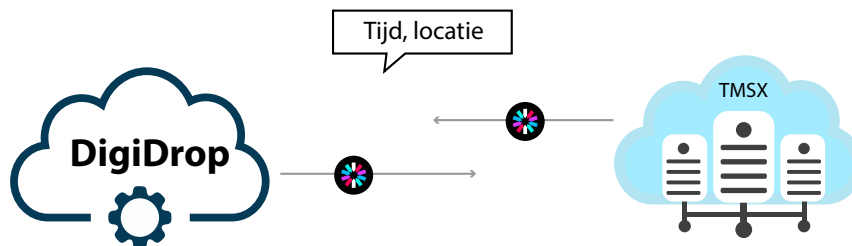
Als dat naar tevredenheid verlopen is krijgt de magazijnmedewerker de vraag 'voer de pincode in': dat is de pincode die de chauffeur via Whatsapp gekregen heeft. De chauffeur geeft die door aan de magazijnmedewerker.<sup>16</sup>



Na invoer van de pincode krijgt de magazijnmedewerker het nodige in de DigiDrop app te zien, zoals:

- Alle checks zijn gedaan.
- Kenteken, ID-chauffeur, transporteur.
- De verkooporder.
- Welke lading opgehaald wordt.

De magazijnmedewerker bevestigt de gegevens in de app: het inladen kan starten.

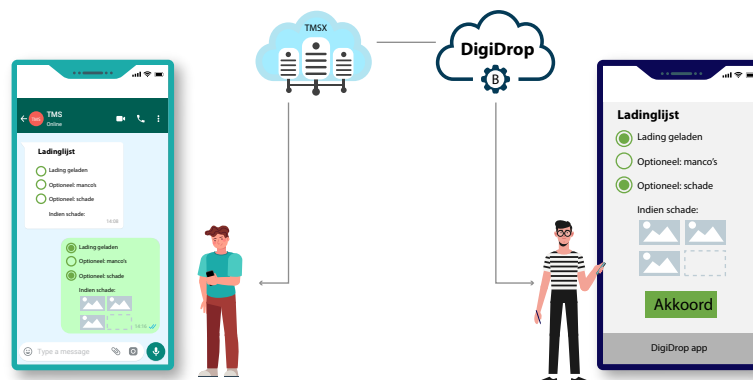


*De DigiDrop provider en TMSX wisselen het digitale bewijs uit van de bevestiging (tijdstip, locatie etc.)<sup>17</sup>*

<sup>16</sup> De pincode voegt weinig toe aan het bewijs maar geeft wel een barrière om privacy gevoelige gegevens te tonen. De chauffeur geeft door het overdragen van de pincode aan de andere medewerker defacto toestemming om de data te zien, waaronder naam, rijbewijs of andere gegevens.

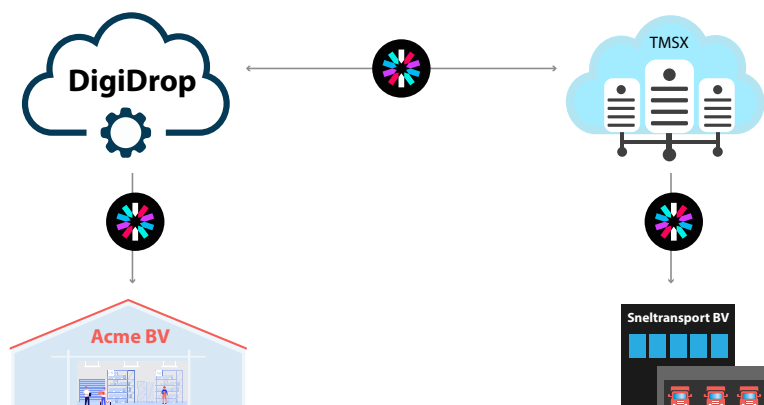
<sup>17</sup> De DigiDrop provider maakt en tekent een JWS die naar TMSX gestuurd wordt.

Na het inladen stuurt TMSX nogmaals de ladinglijst naar de Whatsapp van de chauffeur met de vraag of er opmerkingen, manco's, schade of wijzigingen zijn. Zo ja, dan geeft de chauffeur dat op eventueel met foto's erbij als bewijs.



*TMSX stuurt de ladinglijst met opmerkingen naar de DigiDrop provider*

De DigiDrop provider laat die extra gegevens/opmerkingen/foto's weer zien aan de magazijnmedewerker in de app voor akkoord. De magazijnmedewerker geeft akkoord via de app.

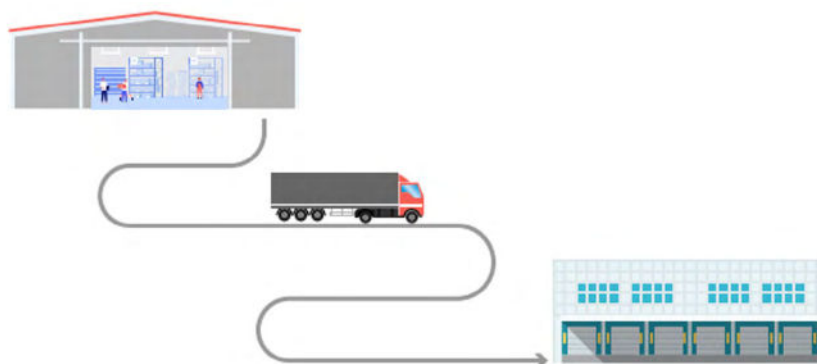


*De DigiDrop provider stuurt TMSX een getekend digitaal bewijs uit van het akkoord.*

*De DigiDrop provider stuurt hetzelfde bewijs door naar Acme BV voor het archief.*

*TMSX stuurt het bewijs door naar Sneltransport BV voor het archief.*

De chauffeur kan daarna op weg gaan naar het afleveradres.



---

## 3.2 Obstakels

### Geen mobiel internet in magazijn

Over het algemeen kan de magazijnmedewerker gebruik maken van de interne wifi maar de chauffeur niet. Als het magazijn veel metaal bevat kan het zo zijn dat de chauffeur binnen het gebouw geen verbinding heeft met het mobiele internet.

Omdat TMSX van tevoren zowel de QR-code als de pincode naar de chauffeur stuurt is het gebrek aan connectiviteit voor die overdracht geen probleem.

Na het inladen heeft de chauffeur wel connectiviteit nodig om manco's, opmerkingen en foto's door te sturen. Voor het maken van de foto's is echter geen internet nodig.

Bij het wederzijds goedkeuren van de opmerkingen hoeven de chauffeur en de magazijnmedewerker niet naast elkaar te staan: dat kan op afstand.

### De magazijnmedewerker kan geen QR-code scannen

Sommige apparaten hebben geen camera of kunnen geen QR-code scannen.

Het alternatief is dat de chauffeur een unieke korte URL in Whatsapp krijgt, een URL die met niet al te veel moeite over te typen is. Er zijn allerlei dienstverleners die URL verkorters leveren. TMSX kan er eentje van gebruiken om een lange specifieke URL die in de QR-code zou zitten te laten omzetten naar een korte unieke (en tijdelijke).

### Het apparaat van de magazijn medewerker is kapot, of heeft geen verbinding

Ook hier biedt de korte URL de oplossing. De magazijn medewerker kan de korte URL overschrijven op papier: om die later te gebruiken, of om door te bellen naar iemand die een PC met een browser heeft (en zo contact legt met de DigiDrop provider). Die persoon op afstand kan de gegevens controleren.

### TMSX is tijdelijk niet bereikbaar

Als de chauffeur al een QR-code (of korte URL) en pincode heeft, kan de magazijnmedewerker in ieder geval die overnemen. Het is dan de partijen om een oplossing te vinden, waarschijnlijk met de telefoon en papier.

## 3.3 Een magazijn heeft geen DigiDrop Provider

Wat nu als de chauffeur bij een magazijn komt waar de medewerkers geen apparaat met een app van een DigiDrop provider hebben, en ze ook geen abonnement hebben op zo'n provider?

Dan is er een terugvaloptie: weliswaar minder beveiligd en zeker, maar nog steeds werkbaar. Zolang het magazijn maar apparaten heeft met een browser en een internetverbinding.

De chauffeur krijgt een tijdelijke pincode en een korte URL in zijn Whatsapp bij aankomst. (Een QR-code kan natuurlijk ook, als het apparaat van de magazijnmedewerker daarmee om kan gaan).

De magazijnmedewerker gebruikt die korte URL in een browser om verbinding te leggen met TMSX. De pincode is om de informatie zichtbaar te maken. De gegevens kunnen doorgemailed of gedownload worden.

---

Na het laden gaat via de dialoog tussen magazijnmedewerker en TMSX via dezelfde browser.

Deze variant is minder zeker dan die met een DigiDrop provider omdat TMSX door het magazijn geheel vertrouwd moet worden. In de praktijk zal het in veel gevallen een acceptabele terugvaloptie zijn.

### **3.4 Opnemen in algemene voorwaarden**

De juridische basis wordt versterkt als de twee betrokken partijen deze werkwijze opnemen in hun algemene voorwaarden: d.w.z. dat deze manier van werken acceptabel is als bewijs van overdracht (commercieel gezien, burgerlijk recht).

De verkoper neemt dit op in zijn algemene voorwaarden van levering aan klanten.

De transporteur neemt dit op in zijn algemene voorwaarden van levering van de transportopdracht.

De verkoper heeft een contractuele overeenkomst met de DigiDrop provider (of regelt dat zelf) waarin de werkwijze en eisen beschreven zijn.

De transporteur heeft een contractuele overeenkomst met TSMX waarin de werkwijze en eisen beschreven zijn.

De ontvanger heeft op zijn beurt ook een contractuele overeenkomst met een (andere) DigiDrop provider (of regelt dat zelf) waarin de werkwijze en eisen beschreven zijn.

## 4 Werkwijze bij aantonen professionele diploma's en certificaten

---

De inhoud van de JWS kan een beschrijving van een bepaald diploma- of professioneel certificaat zijn. Een professionele chauffeur kan bijvoorbeeld zowel een chauffeursdiploma hebben als een aantekening gevaarlijke stoffen. Een servicemonteur kan een diploma hebben om met warmtepompen en koudemiddelen om te mogen gaan. Enzovoorts.

Als die beschrijvingen gestandaardiseerd zijn is daarmee vooraf en naderhand te bewijzen dat de maker van de JWS (de aansprakelijke organisatie) deze bewering gedaan heeft: de persoon die gestuurd is heeft de noodzakelijke 'papieren'.<sup>18</sup>

Op afzienbare termijn zullen digitale bewijzen van deze diploma's of certificaten mogelijk worden: de zogenaamde 'verifiable presentations' van 'verifiable credentials'. Door deze digitale bewijzen van diploma's in de JWS te stoppen wordt nog meer zekerheid verkregen.

Een 'verifiable credentials' (afgekort VC) is nu meestal een digitale variant van een voorheen papieren document. De eerste toepassingen zijn zaken als vliegtickets: bekend als een opgeslagen boarding pass in de 'wallet' (Engels for portefeuille) op een telefoon. Er wordt door overheden gewerkt aan soortgelijke vormen voor digitale rijbewijzen en digitale identiteitsbewijzen.

Een VC kan ook een digitaal bewijs zijn van een vluchtiger iets, zoals het bezit van een bankrekening. Een uitgevende instelling (bank, overheid, opleidingsinstituut etc.) geeft een door hen digitaal getekende VC aan een 'houder', bijvoorbeeld een servicemonteur die een bepaald diploma heeft. De monteur kan de VC tonen aan iemand die zeker wil weten dat de monteur dat specifieke diploma heeft. Het vertrouwen is gebaseerd op de reputatie van de uitgevende instelling.

In zakelijke toepassingen is het belangrijk om te beseffen dat de aansprakelijkheid bij het bedrijf ligt, niet bij de persoon zelf. De persoon bewijst met een VC aan het bedrijf die hem/haar inzet dat hij/zij een geldig diploma heeft, het bedrijf bewijst met de JWS aan de klant dat ze zich aan de afspraken houden, d.w.z. een gekwalificeerd persoon inzetten.

---

<sup>18</sup> Een persoon kan een papieren document als bewijs tonen aan het bedrijf. Het bedrijf geeft een digitaal bewijs aan de klant dat ze ervoor instaan dat deze persoon gekwalificeerd is. Met andere woorden: een deel van de keten kan nog uit papier bestaan: dat maakt het introduceren wel zo makkelijk.

## 5 Toepassen in de praktijk voor toezichthouders

In hoofdstuk 3 en 4 is de uitwerking gegeven voor toepassingen waarbij er een commerciële interactie is tussen bedrijven.

Het blijkt dat hetzelfde mechanisme toepasbaar is voor het leveren van data aan toezichthouders. De eFTI regulering gaat een oplossing bieden voor een deel van de data die toezichthouders vragen. In dit document wordt voorgesteld om:

- Dezelfde technologie (JWS) toe te passen die voor zakelijke commerciële interacties geschikt is
- Een generiek mechanisme te nemen dat voor alle soorten bewijzen in principe geschikt is.

### 5.1 Open 4 corner model bij inspectie

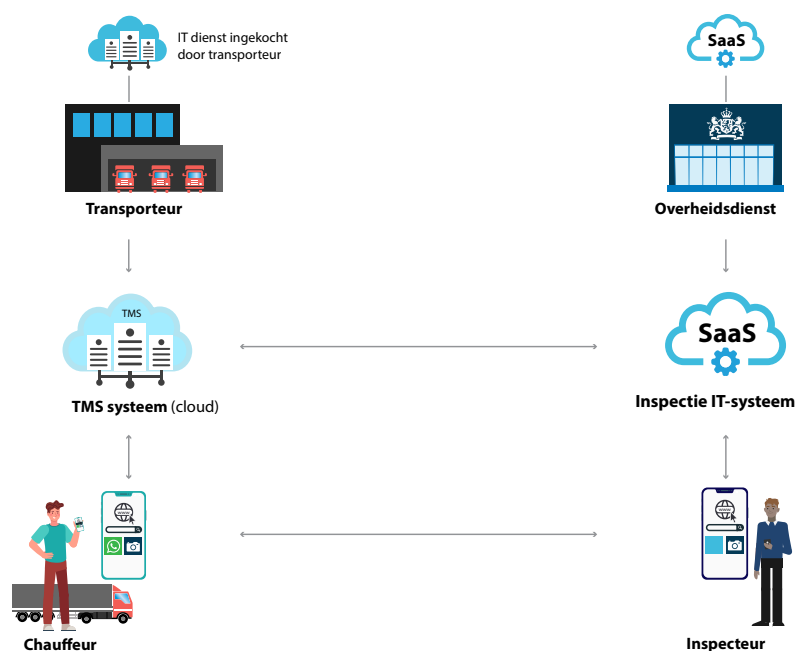
Het aantal wetten en regels rond transport van goederen is aanzienlijk: een deel gaat over het vervoersmiddel en de bestuurder (veilig professioneel transport volgens de regels, maten en gewichten, uitstoot, rij en rusttijden, etc.), het grootste deel gaat over de goederen zelf (heffingen, gevaarlijke goederen, bederfelijke goederen, voedsel, dierlijke oorsprong, etc.).

Overheidsdiensten die toezicht moeten houden op de naleving van die wetten hebben data nodig om hun taak uit te kunnen voeren. Van data in formele meldingen vooraf tot inzicht in documenten en data in IT-systemen bij (fysieke) inspecties, zowel tijdens als na het transport.

Het leveren van data aan een inspectie is schematisch te beschrijven als een open 4-corner model: open omdat de deelnemers aan de 4 hoeken niet gelimiteerd zijn tot een beperkte groep.

De 4 corners worden gevormd door:

- De TMS-dienstverlener namens de transporteur.
- De chauffeur namens de transporteur.
- De IT-systemen van de overheidsinspectie.
- De inspecteur die de fysieke controle uitvoert.



Het uitgangspunt is dat de medewerkers die namens hun organisatie optreden smartphones of tablets hebben met (meestal maar niet continu) connectiviteit: mobiel internet of bedrijfswifi.

De chauffeur heeft een smartphone die geregistreerd is bij de TMS-provider: Simkaart, Mac-adres etc.

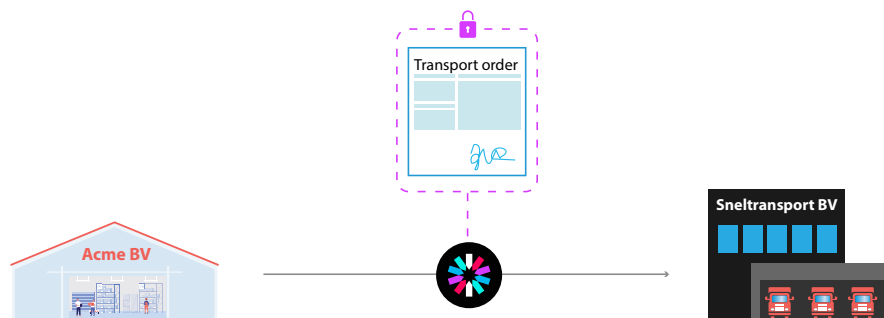
De laagst mogelijke drempel is dat Whatsapp of een andere standaard chat applicatie gebruikt wordt voor de interactie tussen TMS-systeem en de chauffeur.

De inspecteur heeft een mobiel device wat geregistreerd is bij het IT-systeem van de inspectie. De applicatie van de inspectie is geïnstalleerd op het device.

## 5.2 Bewijs leveren aan de inspecteur

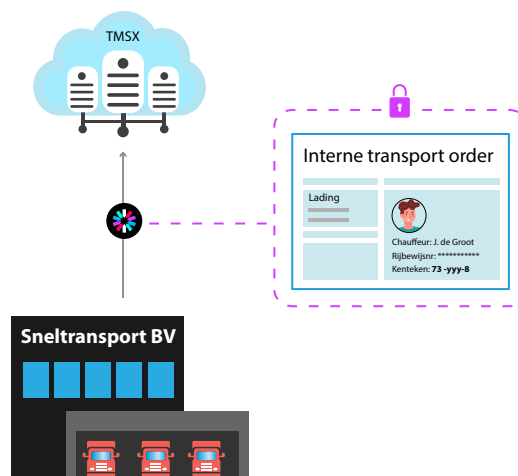
De uitleg gaat aan de hand van een voorbeeld met één zending.

Een handelsmaatschappij (Acme BV) heeft een paar pallets met goederen verkocht en geeft een digitale transportorder aan Sneltransport BV.



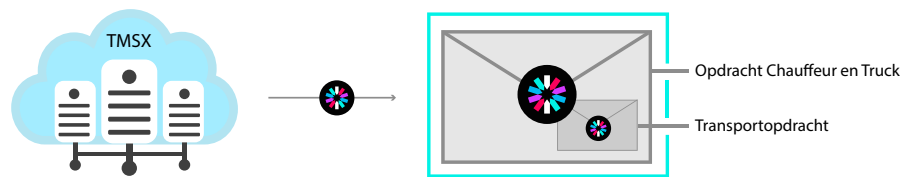
*Acme BV stuurt JWT met de orderinformatie aan Sneltransport BV*

Sneltransport BV maakt gebruik van het Transport Management Systeem (TMS) TMSX, en maakt daarin een interne transportopdracht aan: chauffeur en kenteken van de vrachtwagen zijn nu bekend bij TMSX.



*TMSX ontvangt de Acme JWT van Sneltransport BV.*

De chauffeur heeft een mobiele telefoon met Whatsapp: het nummer en de identiteit van de chauffeur (inclusief ID-nummer) zijn bekend bij TMSX.

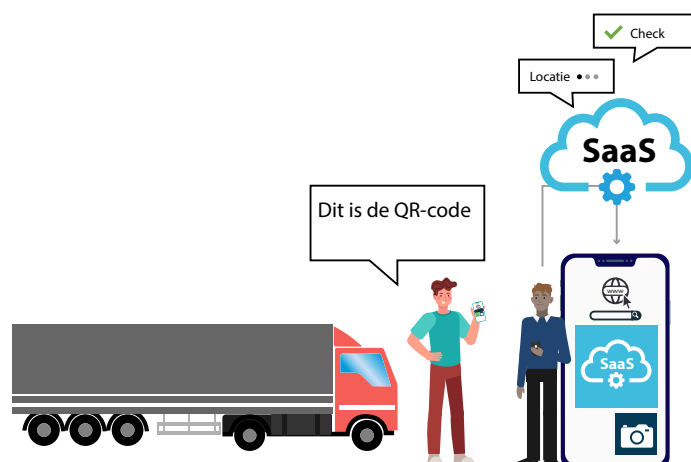


*TMSX creëert een getekend bewijs met de Acme JWS, het bewijs van de vertegenwoordiging van TMSX namens Sneltransport BV en additionele informatie over de vrachtwagen en de chauffeur.*

De chauffeur gaat naar het magazijn van Acme BV toe, haalt de lading op en begint aan zijn rit. Tijdens de rit houdt een inspecteur de vrachtwagen aan en vraagt om gegevens. De chauffeur geeft aan TMSX op dat er een inspectie is.



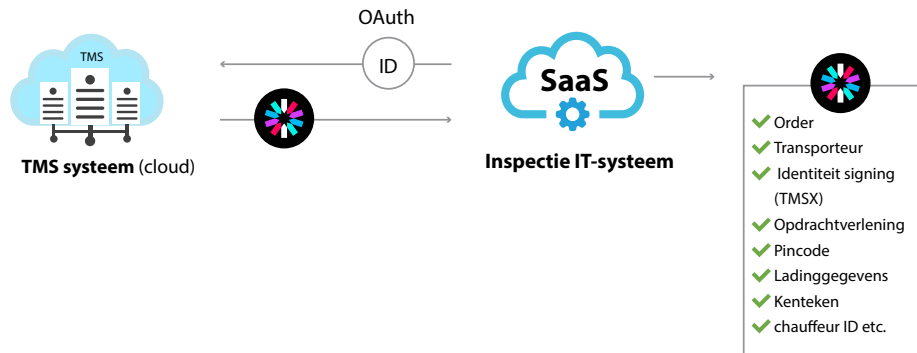
*TMSX verifieert de geolocatie van de telefoon en de vrachtwagen: die moeten bij elkaar in de buurt zijn. TMSX stuurt een tijdelijke QR-code (of een short URL die over te typen is) en een tijdelijke pincode via Whatsapp naar de chauffeur. De QR-code geeft de identiteit van TMSX en de link naar de servers van TMSX gecombineerd met de unieke identifier van deze interactie.*



De inspecteur scant de QR-code met zijn device en de inspectieapp.

Het IT-systeem van de inspectie verifieert:

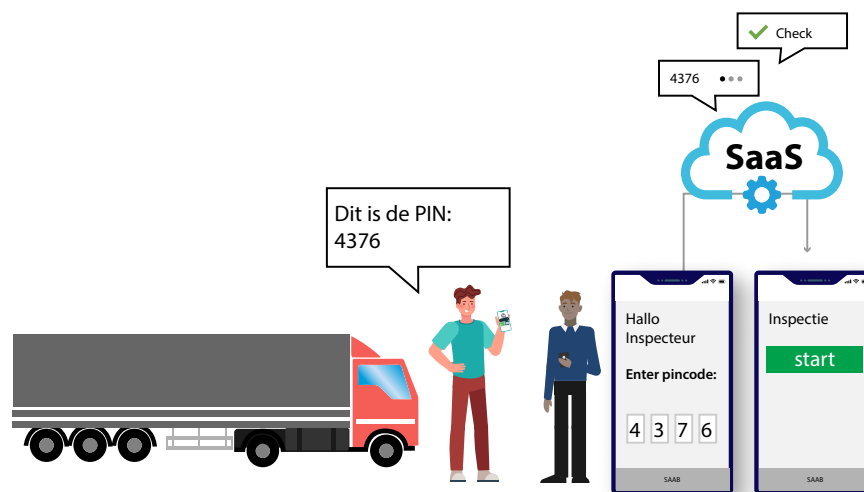
- Locatie device/IP-adres van de inspecteur.
- Identiteit TMSX (digitaal).
  - Bekende en gecertificeerde partij.



Het IT-systeem van de inspectie maakt zich bekend bij TSMX en vraagt de betreffende JWS op.

Het IT-systeem van de inspectie evalueert de JWS:

- Check op orderinformatie en zending.
- Check op transporteur.
- Check op identiteit signing (TMSX).
- Check op opdrachtverlening (wie heeft transporteur ingeschakeld).
- Extractie tijdelijke pincode, ladinggegevens, kenteken, chauffeur ID etc.



Het IT-systeem van de inspectie vraagt de inspecteur om de tijdelijke pincode die de chauffeur moet opgeven. Indien die correct is, wordt de informatie pas getoond in de app van de inspecteur: beveiliging en privacybescherming.

De inspecteur kan vervolgens een controle uitvoeren.

In dit voorbeeld kan de transporteur uit elk land komen: zolang het IT-systeem van de inspectie en TMSX elkaars digitale identiteit vertrouwen werkt de transactie.

Het IT-systeem van de inspectie heeft dezelfde gegevens als de inspecteur, en kan de resultaten van de inspectie meteen verwerken en opslaan.

Een pro-actieve melding aan de inspectie kan op dezelfde manier geschieden, los van een inspectie langs de kant van de weg.

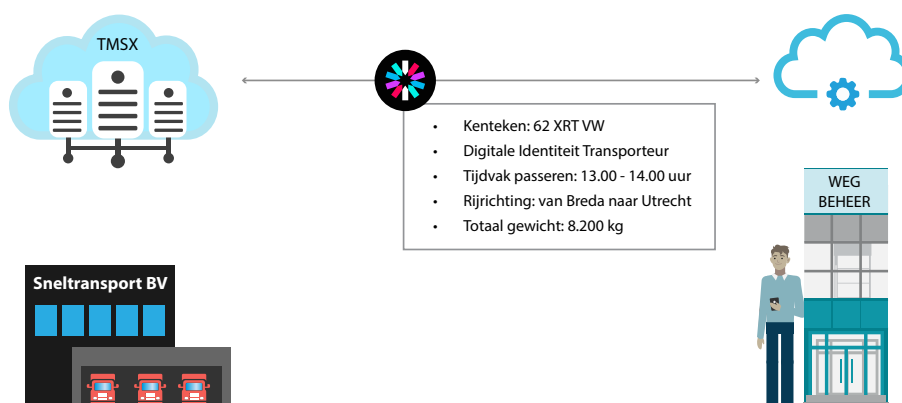
### 5.3 Breder gebruik: privileges

Een verifieerbaar digitaal bewijs kan breder gebruikt worden: bijvoorbeeld om privileges toe te staan en te controleren zoals in het hierna beschreven voorbeeld.

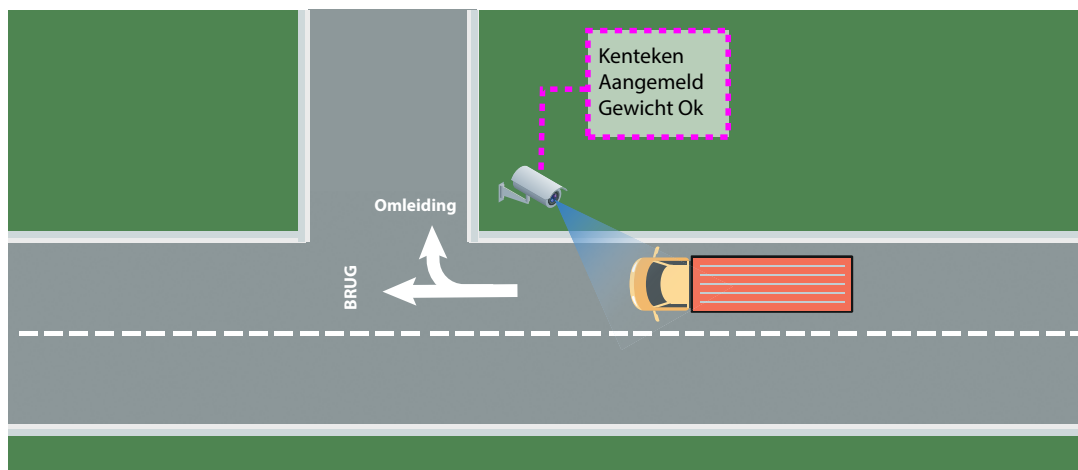
Een van de bruggen in het wegennet vertoont gebreken. De wegbeheerder stelt tijdelijk een gewichtsbepanking in voor vrachtverkeer totdat de herstelwerkzaamheden beginnen. Lege of bijna lege vrachtwagens zouden in principe over de brug mogen maar zwaar geladen vrachtwagens niet.

De werkwijze is dat TMSX namens de transporteur een half uur of meer van tevoren een digitaal bewijs naar de wegbeheerder stuurt, met daarin:

- Het kenteken van de vrachtwagen.
- De digitale identiteit van de transporteur die verantwoordelijk is.
- Het tijdvak waarin de brug gepasseerd gaat worden.
- De rijrichting.
- De declaratie van het totaalgewicht (onder de grens).



De wegbeheerder heeft voor de brug een sluis voor vrachtwagens gemaakt waar een ANPR-camera (kentekenherkenning) de kentekens scant. Een kenteken wat past bij een eerdere geaccepteerde declaratie die nog geldig is mag doorrijden, tenzij besloten is om een controle steekproef te doen. Onbekende kentekens, kentekens met ongeldige bewijzen of vrachtwagens die gecontroleerd gaan worden moeten zijdelings afslaan.



Als een bekend kenteken gepasseerd is (of de geldigheidsduur overschreden is) wordt het digitale bewijs gearchiveerd en de vrijstelling ingetrokken: zo wordt misbruik voorkomen. Transporteurs die misbruik maken van de mogelijkheid kunnen op een zwarte lijst komen. TMSX kan wel een digitaal bewijs insturen maar de declaratie kan geweigerd worden op basis van de identiteit van de transporteur (en/of het kenteken).

Dit voorbeeld laat zien dat de (in elkaar verpakte) JWS een breed toepasbaar mechanisme is.

## 6 Marktwerving

---

De specificatie van JWS is een open wereldstandaard, vrij toepasbaar door iedereen. De softwarebibliotheken om met JWS om te gaan zijn vrij toegankelijk.

Het gebruik van certificaten zoals EIDAS is op zich goed toegankelijk voor iedere professionele partij.

Met het open publiceren van afspraken over de inhoud en de processen is er geen drempel voor partijen om e.e.a. zelf te implementeren.

Gezien de ervaringen met JWS in de huidige praktijk mag verondersteld worden dat het implementeren en onderhouden van IT die dit uitvoert relatief makkelijk en betaalbaar zal zijn. In de praktijk zullen algemene IT-leveranciers, platforms, gespecialiseerde dienstverleners en overheids-IT-diensten hun eigen keuzes maken over het zelf implementeren van dit soort oplossingen of een dienst inkopen bij een SaaS partij.

## 7 Ondersteuning door het BDI-stelsel

Het BDI-afsprakenstelsel ([www.bdinetwork.org](http://www.bdinetwork.org)) ondersteunt de hierboven beschreven werkwijze op verschillende manieren.

### 7.1 Vertrouwen in partijen

De uitgever van een digitaal certificaat (eIDAS, etc.) waarmee een JWS digitaal getekend wordt garandeert de relatie tussen een juridische entiteit (bedrijf, instituut, overheidsdienst) en het certificaat. Die relatie ('diegene die deze digitale handtekening gezet heeft is deze partij') gaat over de identiteit, niet over het (zakelijk) vertrouwen in de partij.

De BDI Association is een lokale decentrale rechtspersoon die alle leden ondersteunt bij het opbouwen van onderling vertrouwen, en van vertrouwen in derden. Het lokale register koppelt identiteit aan vertrouwen. <https://bdinetwork.org/deployment/governance/>.

Als overheden en bedrijven deze (JWS-gebaseerde) werkwijze willen invoeren is het prettig als je kunt verifiëren of de tegenpartij zich aan de afspraken houdt. Als alle partijen lid worden van een BDI Association, de regels ondertekenen en vooraf een paar testen van de techniek doorstaan, kan real-time geverifieerd worden of je met een 'gecertificeerde' partij van doen hebt.

Die real-time check gaat via het zogenaamde Association Register wat de Association bijhoudt.

### 7.2 Gedeelde algemene voorwaarden

In paragraaf 2.4 wordt gewezen op het nut van gedeelde algemene voorwaarden, specifiek geschreven voor deze toepassing. In BDI-termen zijn dit zogenaamde Edge Agreements <https://bdinetwork.org/interoperability/edge-agreements/>.

Leden van een BDI Association kunnen onderling deze voorwaarden afspreken, en dan is er een goede juridische basis. Het is goedkoop en handig om het zo te regelen.

### 7.3 Gedeelde semantiek

De inhoud van het digitale bewijs kent veel vrijheden: enerzijds handig, maar het is voor de toepassing technisch lastig als je geen afspraken maakt over termen en betekenissen.

Het uitgangspunt van het BDI-stelsel is dat er subtiele lokale verschillen zullen zijn in definities: dat zal afhankelijk van sector, taal, cultuur en lokale wetgeving zijn. <https://bdinetwork.org/framework/core-principles/core-principle-6/>.

Een BDI Association (of een groep van BDI Associations) maakt zelf afspraken over standaarden op dit gebied.

### 7.4 Gedeelde services

Een BDI Association kan, als de leden dat willen betalen, een aantal diensten gemeenschappelijk verzorgen: om de kosten te delen of om expertise te delen. Een voorbeeld is de 'DigiDrop provider' dienst, of een register van mandaten van personen.

## 8 Hybride werkwijzen

Het BDI-stelsel houdt rekening met het feit dat in de realiteit lang niet alle partijen in een (internationale) keten al goed gedigitaliseerd zijn. Soms is men niet in staat (financieel of qua expertise) om moderne IT-systemen te implementeren, soms is er sprake van wantrouwen. Data uitwisselen en data-integratie geeft grotere transparantie: niet iedereen ziet daar het voordeel van in.

In de praktijk van transport komt het vaker voor dat een grotere transporteur een charter inschakelt via een tussenpersoon. En misschien wordt dat werk wel weer verder onder-uitbesteed, onzichtbaar voor de transporteur.

De transporteur weet niet veel meer dan dat de transportorder gegeven is en dat een tijd later een papieren vrachtbrief ingeleverd wordt als bewijs van het afhandelen van de order. Als een klant opbelt dat er geen chauffeur is op het afgesproken tijdstip moet de transporteur gaan bellen met de tussenpersoon om erachter te komen wat er aan de hand is.

Het zou al een grote stap vooruit zijn als de overdrachtsmomenten (inladen, lossen) digitaal afgemeld werden, en nog mooier als er digitaal berichten kwamen over vertragingen of problemen. Maar hoe kan dat geregeld worden zonder apps, DigiDrop providers en data-integratie?

Onderstaand worden twee mogelijke werkwijzen beschreven. Die werkwijzen zijn voorbeelden van zogenaamde 'Edge Agreements' in het BDI stelsel: hybride werkwijzen om de brug te slaan met de 'niet-zo-digitale' werkelijkheid.

De eerste beschreven werkwijze is zo eenvoudig mogelijk gemaakt, maar levert wel digitale events op voor alle betrokkenen: het inladen en het afleveren.

De tweede geeft iets meer mogelijkheden maar vraagt ook wat meer van de gebruikers.

### 8.1 Edge Agreement DigiDrop UltraLite

TMSX is het TMS systeem wat de hoofdtransporteur gebruikt. De uit te besteden transportorders worden in TMSX aangemaakt.

TMSX genereert per zending drie unieke codes, elk van 4 letters.

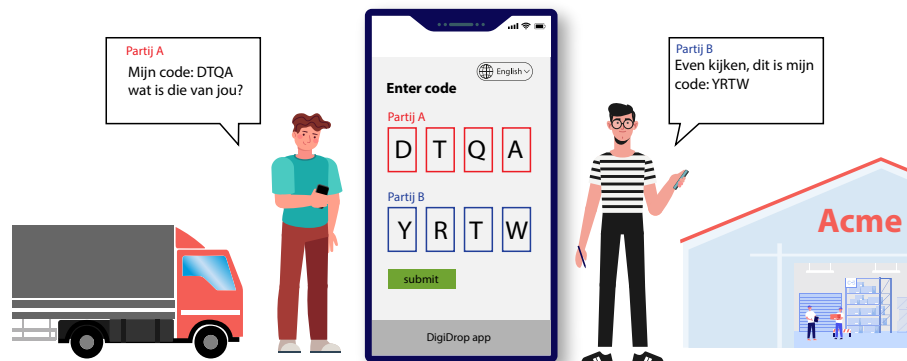
- Bijv. 'DTQA', naar de charter met de transportorder voor de zending mee. De charter geeft de order en de code aan de chauffeur.
- Bijv. 'YRTW', die gaat naar het magazijn waar de zending ingeladen gaat worden.
- Bijv. 'PGHF', die gaat naar de ontvangende klant toe gekoppeld aan de zending/bestelling.

TMSX stuurt de twee combinaties ( DTQA+YRTW, en DTQA+PGHF) naar de website [www.digidrop.online](http://www.digidrop.online) met een link terug naar TMSX. TMSX heeft de data, de website is alleen een makkelijke standaard manier voor gebruikers om de codes in te voeren.

De transportorder wordt via een (papieren) CMR meegegeven aan de charter.

Als de chauffeur de zending komt ophalen, wordt (door of de chauffeur of de magazijn medewerker) de website [www.digidrop.online](http://www.digidrop.online) geopend, liefst mobiel.

Daar voeren ze elk hun 4 letters in, samen 8. (DTQA YRTW) <sup>19</sup>.



De website herkent aan de hand van die 8 letters welke zending het is, welke stap in het proces, en dat TMSX de partij is die het afhandelt.

TMSX laat een paar gegevens over de order zien, als dubbelcheck.

In de meest minimale vorm wordt de overdracht gemeld door een knop in te drukken. Een iets fraaiere variant is als er opmerkingen en foto's toegevoegd kunnen worden (mobiele telefoon).



TMSX kan vervolgens de opdrachtgevers digitaal melden dat de zending ingeladen is.

Bij het afleveren van de zending op de bestemming is het proces identiek.

De voordelen van deze aanpak zijn:

- De code kan desnoods op papier meegenomen en doorgegeven worden.
- Wantrouwige tussenpersonen en charters 'lekker' geen voor hen gevoelige informatie.
- De overdrachtmomenten komen real-time digitaal beschikbaar.
- Het proces werkt parallel aan papieren vrachtbrieven.

<sup>19</sup> Het is eenvoudig om verwisseling van volgorde af te vangen

## 8.2 Edge Agreement Digidrop Lite

Met een relatief simpele uitbreiding kan er meer digitale zichtbaarheid over het verloop van het proces en de planning gerealiseerd worden.

TMSX genereert per zending nu drie unieke codes, elk van 4 cijfers en 4 letters.

- Bijv. '0357 DTQA', naar de charter met de transportorder voor de zending mee. De charter geeft de order en de code aan de chauffeur
- Bijv. '0668 YRTW', voor het magazijn waar de zending ingeladen gaat worden
- Bijv. '0890 PGHF', voor de ontvangende klant gekoppeld aan de zending/bestelling

Een chauffeur kan met zijn code '0357 DTQA' via [www.digidrop.online](http://www.digidrop.online) onderweg berichten sturen over bijvoorbeeld vertragingen en een nieuwe ETA.



De code '0357 DTQA' invoeren geeft op de website simpele dialoog mogelijkheden, zoals 'nieuwe aankomst tijd 16.30 - 18.30 u' in een tekstveld. Dat is 'veilig' voor wantrouwende partijen want er lekt niets over wie deze aanpassing doet.

TMSX krijgt de update door en kan die digitaal doorgeven.

Het magazijn of de ontvangende klant kunnen hetzelfde proces gebruiken om informatie op te halen: 4 cijfers en 4 letters invoeren geeft de status van de zending.

De afhandeling van het melden van de overdracht is gelijk aan de UltraLite versie: 2 x 4 letters invoeren en afmelden.

Deze voorbeelden laten zien hoe een hybride proces ontworpen kan worden om de brug te slaan tussen de wereld waar de voordelen van data integratie met volwassen IT-systemen benut worden en de partijen waar IT-integratie nog niet zover is ontwikkeld is.

## Bijlage 1: JWS en QR-codes

---

In de beschreven werkwijze krijgt de chauffeur een QR-code mee die vooral uit een unieke link naar (in dit geval) TMSX bestaat.

In principe is het ook denkbaar dat de chauffeur de hele JWS bij zich draagt in zijn device. Echter, QR-codes hebben een beperking in de hoeveelheid data die daarin verpakt kan worden. JWT's die in elkaar verpakt zijn vergroten de hoeveelheid data snel tot boven de grens wat nog realistisch te doen is met een QR-code in de praktijk van alledag.

In principe zouden in dat geval andere overdrachtsmethodes in te zetten zijn: NFC overdracht of Bluetooth hebben die beperking niet. Het nadeel daarvan is dat het op de werkvloer veel meer vraagt aan apparatuur en personeel om de gegevensoverdracht betrouwbaar te laten werken.

Een JWS met links naar andere 'verpakte' JWS is veel kleiner. Die zou in een QR-code passen. Het nadeel van deze optie is dat er meer online checks bij allerlei partijen nodig zijn bij het verifiëren van de JWS.

Een van de voordelen van een QR-code met alleen een unieke link is dat die als korte URL over te schrijven is op een stuk papier: handig als er wat mis gaat.

Met de keuze om alleen een link via een QR-code over te dragen wordt de bulk van de complexe IT-interacties naar professionele partijen 'in de cloud' verschoven, ten voordele van de eenvoud en robuustheid op de werkvloer.

## Bijlage 2: Relevante IT-standaarden

---

De JSON Web Signature (JWS) ([RFC 7515 - JSON Web Signature \(JWS\)](#)) beschrijft hoe een generieke 'payload' digitaal getekend overgedragen kan worden, in een JSON formaat.

De JSON Web Token (JWT) ([RFC 7519: JSON Web Token \(JWT\) RFC 9493 - Subject Identifiers for Security Event Tokens](#)) beschrijft de specifieke versie van een JWS om 'claims' te verzenden. Claims zijn als eerste gericht op vertrouwen in identiteiten.

Omdat de normaal gebruikte Base64 encoding soms nadelen heeft, vooral bij het 'embedden' van JWS's en bij grote 'payloads' is er een versie van een JWS die dit nadeel omzeilt (<https://www.rfc-editor.org/rfc/rfc7797.html>).

Bij grote 'payloads' zoals foto's is het voordelig om de foto niet in de JWS in te sluiten: alleen de 'hash' en een identificatie worden in de JWS/JWT meegenomen, de foto wordt bijgesloten.

De ETSI standaard 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](https://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf)) standaardiseert ZIP-files voor het combineren van deze zogenaamde detached signatures met hun gehashte documenten.

In het Europese domein is er aandacht besteed aan de standaardisatie van JWT-velden voor e-signatures en e-seals, o.a. om de betrokken signer te identificeren.

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

Er zijn zogenaamde 'trust lists' die het makkelijk maken om vertrouwen in certificaten te bepalen.

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

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

De benadering is compatibel met de principes voorgesteld door het 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](http://www.bdinetwork.org) | [www.topsectorlogistiek.nl](http://www.topsectorlogistiek.nl) | [www.datainlogistics.org](http://www.datainlogistics.org)

