Dossier elektronische handtekening strafrecht

Begeleiding van invoer in het strafrecht

Klik hier om naam in te voeren

Definitief

Versie 1.0

Versie datum 23 november 2020

Rubricering **Niet Vertrouwelijk**

« waakzaam en dienstbaar »

Inhoudsopgave

Inleiding

U heeft één of meerdere door de politie opgestelde documenten ontvangen die voorzien zijn van een elektronische handtekening. De politie is bezig haar processen te digitaliseren. Daarbij ontstaan steeds meer documenten van de politie alleen nog digitaal, waarmee politie van begin tot eind alleen in digitale vorm wordt gewerkt. Deze documenten worden indien aan de orde voorzien van een elektronische handtekening en gedeeld met belanghebbenden, zoals onze ketenpartners en de rechtspraak. Dit document geeft u informatie over de elektronische handtekening van de politie. U krijgt informatie over:

- de door de politie gehanteerde vorm van de elektronische handtekening;
- de onderliggende waarborgen die zijn ingericht om te voldoen aan de vereisten voor documenten met een elektronische handtekening;
- hoe u de handtekening kunt valideren op echtheid;
- het proces van het ondertekenen; en
- manieren van leveren van getekende stukken.

Op verschillende manieren zijn de authenticiteit en integriteit van een document (met daarin de handtekening(en) van politiemedewerkers of burgers) te valideren. Hierdoor is zichtbaar of het document inderdaad ongewijzigd is sinds de plaatsing van de handtekening. De elektronische handtekening die de politie hanteert voldoet aan alle voorgeschreven wet- en regelgeving, in zowel het bestuursrecht als in het strafrecht. De elektronische handtekening is met diverse waarborgen omkleed, waardoor zij op unieke wijze aan de ondertekenaar is verbonden en de ondertekenaar geïdentificeerd kan worden. De handtekening komt tot stand met gegevens onder de uitsluitende controle van de ondertekenaar. Dit geschiedt door toepassing van de zogeheten twee-factor authenticatie, de visuele kenmerken in/op het document en de vermelding in het zogeheten zegel. De gegevens over de ondertekening zijn op zodanige wijze verbonden aan het getekende document dat eventuele wijzigingen achteraf kunnen worden achterhaald. De elektronische handtekening en de gegevens in het document zijn daarmee eenvoudiger en volledig er te valideren dan de traditionele 'natte handtekening' op papieren documenten.

Bestuursprocesrecht: geavanceerd elektronische handtekening

De vorm van de elektronische handtekening die de politie gebruikt, heet in het bestuursprocesrecht de 'geavanceerde elektronische handtekening', zoals gedefinieerd in artikel 3, onderdeel 11, van de Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 (hierna: eIDAS verordening). De geavanceerde elektronische handtekening voldoet aan de eisen in artikel 26, eIDAS verordening en is omkleed met diverse waarborgen, die er mede voor zorgen dat de handtekening voldoet aan artikel 2:16 eerste en tweede lid Algemene wet bestuursrecht. De belangrijkste waarborgen zijn:

- twee-factor authenticatie bij de ondertekening, die garandeert dat de ondertekenaar identificeerbaar is en zijn/haar identificerende gegevens inclusief de gegevens over de ondertekening op unieke wijze verbonden zijn aan het elektronische document;
- verzegeling met een gekwalificeerd elektronisch zegel (als bedoeld in artikel 3, onderdeel 27, eIDAS verordening). Het zegel is onder andere gebaseerd op een gekwalificeerd certificaat (als bedoeld in artikel 3, onderdeel 30, eIDAS-verordening); en
- het certificaat (onder het zegel) waarborgt de authenticiteit en integriteit van het getekende document en de handtekening in het document; het certificaat is niet de handtekening zelf: het certificaat en de zegel zijn op Politie-organisatieniveau; de handtekening is op persoonsniveau binnen het document.

Jurisprudentie

Op 8 oktober 2019 heeft de Afdeling bestuursrechtspraak van de Raad van State uitspraak gedaan in een zaak waar stukken zaten die voorzien zijn van de hier genoemde elektronische handtekening. Deze werkwijze is door deze hoogste bestuursrechter geaccepteerd. De uitspraak is te vinden onder nummer ECLI:NL:RVS:2019:3355.

Strafprocesrecht: Elektronische handtekening

De elektronische handtekening is ook geschikt voor toepassing in het strafprocesrecht:

- de handtekening voldoet onder meer aan de eisen inzake authenticatie, zoals vereist op grond van artikel 5 Besluit digitale stukken Strafvordering. Dit betekent dat het authenticatie-middel dat de politie inzet voor het zetten van de elektronische handtekening is uitgegeven door de politie, is aangewezen op grond van een Besluit van de korpshef (bijlage Aanwijsbesluit authenticatiemiddel t.b.v. ondertekenen) en dat deze uitgaat van een tweefactor (of hoger) authenticatie middel.

- de elektronische handtekening bestaat uit elektronische gegevens die gehecht zijn aan of logisch verbonden zijn met andere elektronische gegevens, en die worden gebruikt door de ondertekenaar om te ondertekenen (artikel 138e Wetboek van Strafvordering - Sv);
- onder 'getekend of ondertekend' (…) wordt mede verstaan een ondertekening (…) met een elektronische handtekening die voldoet aan de bij of krachtens algemene maatregel van bestuur te stellen eisen ten aanzien van in elk geval het betrouwbaarheidsniveau van authenticatie (artikel 138f Sv);
- van een processtuk in elektronische vorm kan de integriteit worden nagegaan doordat iedere wijziging daarvan kan worden vastgesteld (art. 149a, derde lid, Sv). De elektronische handtekening is ook in te zetten voor ondertekening door burgers middels de zogeheten tablethandtekening als omschreven in artikel 6, tweede lid, Besluit digitale stukken Strafvordering:
  "2. De elektronische handtekening, bedoeld in artikel 138e van de wet, zijnde een handgeschreven handtekening op een elektronische gegevensdrager, voldoet aan de volgende eisen:
  a. de ondertekening heeft plaatsgevonden in aanwezigheid van of wordt gedaan door:
  – een rechter of griffier;
  – de bevoegde ambtenaar, bedoeld in artikel 163, eerste lid, van de wet met het oog op de aangifte of klacht, bedoeld in artikel 161 van de wet, en
  b. de biometrische of grafische handtekening is op zodanige wijze aan de elektronische gegevens waarop zij betrekking heeft verbonden, dat het moment van ondertekening en elke wijziging na ondertekening van de elektronische gegevens kan worden vastgesteld."

Jurisprudentie
Op 20 december 2018 heeft de Rechtbank Rotterdam een strafvonnis gewezen in een zaak waarvan het procesdossier via de Digitaal Proces Dossier (DPD) applicatie was opgesteld en waarin stukken zaten, voorzien van de hier genoemde elektronische handtekening. Deze werkwijze is door deze rechter geaccepteerd. De rechterlijke uitspraak is te vinden onder nummer ECLI:NL:RBROT:2018:10537. Eerder heeft de rechtbank over een DPD-zaak met tablethandtekeningen beslist. Deze uitspraak is te vinden onder nummer ECLI:NL:RBROT:2017:8531.

1. Waarborgen voor de elektronische handtekening

De elektronische handtekening van de politie is omkleed met de vereiste waarborgen. Deze waarborgen zien er in samenhang op toe, dat iedere betrokkene kan vertrouwen op het gegeven dat de handtekening is gezet door enkel diegene die in het document staat vermeld, dat de authenticiteit en integriteit van het document in orde zijn en dat deze op ieder gewenst moment zijn na te gaan. Daarmee biedt de elektronische handtekening in feite zelfs meer zekerheid dan de traditionele 'natte handtekening'. Alle ingerichte waarborgen worden hieronder nader omschreven.

1.1. Twee-factor-authenticatie: hebben & weten

De elektronische handtekening wordt gezet door de politiemedewerker via een door de politie op de persoon verstrekte diensttelefoon. Er wordt gebruik gemaakt van een geauditeerd en geprotocolleerd uitgifte-proces om diensttelefoons op de persoon uit te reiken. De uitgifte wordt in een uitgifte-administratie vastgelegd. Meer details over het uitgifteproces zijn opgenomen in bijlage (Uitgifteproces diensttelefoon). Door middel van een Onderteken-app die zich in de beveiligde omgeving op de diensttelefoon bevindt kan de politiemedewerker een ondertekening uitvoeren. De politiemedewerker logt in op zijn diensttelefoon met een wachtwoord en vervolgens op de beveiligde omgeving met een pincode of door het aanbieden van zijn/haar vingerafdruk. Deze gegevens zijn enkel bij de politiemedewerker bekend. Met de combinatie van een op de persoon verstrekte diensttelefoon, een inlog op de diensttelefoon en een beveiligde omgeving met de Onderteken-app, komt de handtekening tot stand met gegevens die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken. De ondertekenaar is hiermee identificeerbaar en op unieke wijze verbonden aan de elektronische handtekening.

1.2. Visuele uitingen in en op het document

Documenten die de politiemedewerker in elektronische vorm ondertekent, zijn voorzien van visuele kenmerken in en op het document. Zo is de opzet van de weergave soortgelijk aan hoe de "natte handtekening" wordt weergegeven. In het geval dat een burger een tablethandtekening plaatst (onder toezicht van de politiemedewerker), wordt de door de burger geplaatste handtekening/paraaf weergegeven op het document (art. 6 Besluit digitale stukken Strafverordening). Als de politiemedewerker elektronisch ondertekent, wordt in plaats van de traditionele 'natte krabbel' de regel 'Elektronisch ondertekend op <datum>' weergegeven op het document.

In bepaalde gevallen maakt de politie de elektronische handtekening(en) zichtbaar op een daarvoor ingericht zogeheten 'tekenblad'. Dit is een in het document gevoegde laatste pagina, die daarmee onderdeel vormt van het document. Het tekenblad maakt het mogelijk de elektronische handtekening weer te geven op documenten, wanneer dit binnen bestaande formulieren niet in te voegen valt. Zoals het geval bij oudere (zogenaamde 'legacy') of kant-en-klare niet te wijzigen ICT-applicaties.

Daarnaast wordt ieder door de politiemedewerker in elektronische vorm ondertekend document voorzien van een uniek documentkenmerk in de metadata van het document, als ook het Organisatieidentificatienummer (OIN) van de politie. Zie bijlage (Visuele kenmerken in / op het document) voor een toelichting over het inzien van deze metadata.

1.3. Opslag in associatie-record

Zodra een document is ondertekend, wordt een zogeheten associatie-record gecreëerd. De associatie-record bevat gegevens over wie wanneer in welke hoedanigheid en namens welke organisatie een ondertekenhandeling op het betreffende document heeft uitgevoerd. Dit record is door middel van tenminste één hash-waarde (een versleutelde code, berekend over het getekende document) onlosmakelijk verbonden met het getekende document. Door de hash-waarde op een later moment opnieuw te berekenen, kan worden nagegaan of het document sinds de ondertekening ongewijzigd is.

1.4. Toepassing gekwalificeerd elektronisch zegel

Als additionele waarborg past de politie een gekwalificeerd elektronisch zegel (als bedoeld in artikel 3, onderdeel 27, eIDAS verordening) toe bij iedere elektronische handtekening die wordt geplaatst. Het zegel is onder andere gebaseerd op een gekwalificeerd certificaat (als bedoeld in artikel 3, onderdeel 30, eIDAS-verordening). Zie ook bijlage (Accreditatie verklaring certificaat leverancier). Tijdens iedere toepassing van het zegel worden de belangrijkste functionele gegevens over de ondertekenaar (zoals vastgelegd in het eerder genoemde associatie-record) óók onlosmakelijk verbonden met het document zelf. Vanwege de cryptografische eigenschappen van een gekwalificeerd zegel, dat gebaseerd is op een gekwalificeerd certificaat, en de validatie functie in de gangbare PDF-

viewers wordt direct opgemerkt als een document na toepassing van het zegel is gewijzigd. Daarmee is de authenticiteit en integriteit van het document en (de) daarin vastgelegde elektronische handtekening(en) gewaarborgd. Het elektronische zegel is dus geen vervanging van de elektronische handtekening. Het is één van de waarborgen onder de (geavanceerde) elektronische handtekening. In tegenstelling tot bijvoorbeeld de Koninklijke Marechaussee en het Openbaar Ministerie, hanteert de politie een elektronisch zegel op organisatieniveau. Mede om die reden betreft de elektronische handtekening van de politie ook een 'geavanceerde' en niet een 'gekwalificeerde' elektronische handtekening. De eIDAS verordening stelt aan de geavanceerde handtekening dus ook niet de eis om elektronische certificaten op persoonsniveau te gebruiken, omdat een geavanceerde elektronische handtekening toereikend met diverse (andere) waarborgen is omkleed.

1.5. Audits en penetratietesten

De politie laat de Ondertekenvoorziening en omringende processen auditeren (Zie: onderdeel 3.4 van de Nota van toelichting bij het Besluit digitale stukken Strafvordering). Zo wordt getoetst en daarmee extra gewaarborgd dat de vereiste procedures worden gevolgd, de aangebrachte waarborgen onder de handtekeningvorm in stand blijven en dat de elektronische handtekening binnen de ketens van de werkprocessen van de politie correct wordt geïnterpreteerd. Daarnaast wordt jaarlijks een zogeheten 'penetratietest' uitgevoerd op de Ondertekenvoorziening. Hiermee wordt de beveiliging van de software en hardware van de voorziening onderworpen aan een breed scala van inbraakpogingen.

2. Valideren van een elektronisch ondertekend document

Een door de politiemedewerker elektronisch ondertekend document kan op twee manieren worden gevalideerd; validatie met gangbare PDF-weergave software (PDF-viewer) en validatie met de Gemeenschappelijke Authenticatie, Associatie en Validatieservice (GAAV).

2.1. Validatie met GAAV

Validatie met GAAV

Elektronisch ondertekende documenten van de politie kunnen onafhankelijk gevalideerd worden via de Gemeenschappelijke Authenticatie, Associatie en Validatieservice (GAAV) van de Justitiële Informatiedienst. De dienst GAAV is te raadplegen via https://validatie.justid.nl en stelt een ieder in staat om na te gaan of digitale documenten die zijn uitgegeven door de politie authentiek en integer zijn volgens de geldende regels. Daarmee ontstaat desgewenst extra zekerheid over de afkomst en ongewijzigde staat van deze digitale stukken. Een ieder die over het digitale document beschikt, kan de authenticiteit en integriteit hiervan dus onweerlegbaar controleren via GAAV. Via het GAAV portaal dient het digitale document geüpload te worden, waarna GAAV de authenticiteit en integriteit van het document controleert. Het document dat geüpload wordt, moet een digitaal origineel zijn: het mag geen scan zijn van een geprint document. Een scan van een geprint document bevat immers niet meer de eigenschappen die validatie van de handtekening mogelijk maken. Nadat GAAV het document heeft gecontroleerd wordt het validatierapport direct aan de gebruiker getoond. Indien het document authentiek en integer is bevonden, dan ziet de gebruiker dat weergegeven. Indien het document niet bekend is bij GAAV of volgens GAAV niet integer wordt geacht, dan dient de gebruiker contact op te nemen met de instantie die aan de gebruiker het document heeft verstrekt. De procedure voor een GAAV-validatie is beschreven in bijlage (Validatie).

2.2. Validatie met PDF-viewers

Gangbare PDF-viewers ondersteunen het valideren van het in het PDF-document toegepaste certificaat. Wel kan het zijn dat PDF-viewers verschillend werken en onderling afwijkend omgaan met uitingen rondom de authenticiteit en integriteit. In het rechtsverkeer wordt een stand-alone (niet binnen een web-browser) en actuele installatie van Adobe Reader voorgeschreven. De keuze voor inzet van een bepaalde PDF-viewer is de verantwoordelijkheid van de gebruiker. Wanneer een gebruiker een andere PDF-viewer (zie ook: https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/wat-is-een-elektronische-handtekening) gebruikt en toch wil valideren, dient deze zich te vergewissen van hoe online validatie gaat van documenten voorzien van een certificaat. Bijlage (Validatie) bevat een toelichting over de validatie met behulp van Adobe Reader.

3. Proces van elektronisch ondertekenen

Politiemedewerkers hebben toegang tot vaste en mobiele werkplekken (zoals de diensttelefoon / telewerkplek). Daarop inloggen verloopt altijd via de daartoe ingerichte veiligheidsmaatregelen. Tot de vaste werkplek komt men altijd door eerst een gebouw te betreden en door toegangspoortjes te gaan. Om met de vaste werkplek te komen tot de werkomgeving, waar specifieke applicaties beschikbaar komen, dient men in te loggen met gebruikersnaam en wachtwoord. Tot de werkomgeving via telewerken komt men door zogeheten op tweefactorbasis te authentiseren (DigiPass). Tot de werkomgeving op de diensttelefoon komt men door de diensttelefoon te ontgrendelen en in te loggen in de extra beveiligde omgeving (ingeven pincode of aanbieden vingerafdruk).

Aangekomen in de werkomgeving van de politie heeft de politiemedewerker de beschikking over applicaties, waaronder procesapplicaties. Deze applicaties zijn enkel toegankelijk voor daartoe geautoriseerde politiemedewerkers en zet men in om het werkproces te ondersteunen, zoals het opmaken van processen-verbaal door een opsporingsambtenaar. Bij het opmaken van documenten kan men aangeven wie het document moeten ondertekenen. Op het moment dat de politiemedewerker toe is aan het formaliseren / afsluiten van het document door middel van het plaatsen van zijn elektronische handtekening, initieert hij een tekenverzoek vanuit de desbetreffende applicatie. Zoals door te klikken op een knop “Aanbieden voor ondertekening”. Het tekenverzoek zal op de diensttelefoon van de politiemedewerker verschijnen. Deze diensttelefoon is aan de politiemedewerker in persoon uitgereikt en op zijn naam geregistreerd (“hebben”). Op deze diensttelefoon logt hij in met zijn persoonlijke wachtwoord (“weten”). Vervolgens logt hij met een wachtwoord, pincode of door aanbieden van vingerafdruk in op de beveiligde omgeving op deze diensttelefoon (“weten/zijn”). Op deze wijze is de identiteit van de ondertekenaar via multi-factor-authenticatie geverifieerd. De politiemedewerker klikt op de tekenverzoek-melding, en zo opent de ondertekenapplicatie. Daarin staat het desbetreffende ondertekenverzoek behorende bij het te ondertekenen document. Hij kan op zijn diensttelefoon het document indien gewenst nogmaals bekijken, ondertekenen of de ondertekening weigeren.

In het geval een burger moet ondertekenen, dient dat uitgevoerd te worden onder toezicht van de politiemedewerker (art. 6 Besluit digitale stukken Strafverordening). De politiemedewerker valideert eerst de identiteit van de burger, opent het 'burger-ondertekenvenster' in de Onderteken-app en biedt zijn diensttoestel aan de burger aan. De burger kan er voor kiezen het elektronische document in te zien alvorens de tablethandtekening op de diensttelefoon te plaatsen. De burger kan er ook voor kiezen om ondertekening te weigeren.

Met het klikken op de "Ondertekenen"-knop op de diensttelefoon wordt het proces van digitaal ondertekenen uitgevoerd: Het document wordt voorzien van de elektronische handtekening met daarbij behorende gegevens van de politiemedewerker/burger en diverse waarmerken. Het belangrijkste waarmerk is de verzegeling van het document en de daarbij onlosmakelijk vastgelegde gegevens over de ondertekening: door middel van een gekwalificeerd elektronisch zegel van de politie. Hierdoor zijn het document en de elektronische handtekening onlosmakelijk met elkaar verbonden.

Na ondertekenen komt het document beschikbaar in de procesapplicatie en kan de politiemedewerker daarmee het werkproces vervolgen. Zoals een los document verstrekken aan de burger, of een procesdossier vormen en overdragen aan het Openbaar Ministerie (OM).

4. Overdracht procesdossier met getekende documenten

De politie werkt steeds meer volledig digitaal, vanaf het begin op straat tot het digitaal leveren aan keten partners. Dit omvat echter een transitie waarbij bepaalde processen digitaal gaan en andere processen nog met papier verlopen. Uiteindelijk worden digitale dossiers gevormd, ook door bijvoorbeeld het overgebleven papier onder Vervanging om te zetten naar digitale originelen. Ook speelt mee dat naast de politie ook haar ketenpartners als OM en Rechtspraak, in transitie zijn naar volledig digitaal werken. Daarbij hanteren ketenpartners een eigen snelheid en werken op verschillende procesdomeinen toe naar digitaal werken. Logischerwijs zijn er daarom perioden van het papier-naar-digitaal omzetten (scannen onder Vervanging), dan wel digitaal-naar-papier omzetten (printen).

De politie zet ten minste de navolgende twee kanalen in voor het leveren van het procesdossier aan het OM. Eén papieren en één digitaal kanaal. Hieronder wordt nader toegelicht hoe de overdracht van het procesdossier verloopt.

4.1. Elektronische overdracht

Elektronische overdracht heeft de politie vormgegeven in de DPD-applicatie. Deze applicatie verlengt processystemen, zoals de applicaties BVH en OPP, en ondersteunt daarmee dit onderdeel van het primaire politieproces. Als het onderzoek is afgerond worden door de dossiervormer van de politie alle documenten in de DPD-applicatie geselecteerd die samen het digitale procesdossier moeten vormen. In het geval papieren documenten ontbraken, worden deze bij in het dossier gescand en eveneens in de selectie ten behoeve van het procesdossier opgenomen. De dossiervormer controleert het dossier op tal van kwaliteitsaspecten en zorgt er voor dat deze voldoet aan de ketenkwaliteitscriteria, zoals vastgesteld op 22 oktober 2020 door het Platform Opsporing en Vervolging VVC.

Vervolgens wordt in de beginfase van invoer van de elektronische handtekening door de politie een informatieve brochure opgenomen in het procesdossier. Deze bevat een samenvatting van het dossier van de politie als het gaat over de werkwijze van het gebruik van de elektronische handtekening in het betreffende dossier. De brochure is opgenomen in bijlage (Brochure Elektronisch ondertekenen in de strafrechtketen).

Vervolgens stuurt de dossiervormer van de politie met een druk op een knop het digitale procesdossier elektronisch over naar het OM. Dat verloopt via de voorziening Elektronisch Berichtenverkeer (EBV) en met inzet van de zijde van de politie van een zogeheten Elektronische Politie Broker (EPB). De EPB is een infrastructuur voor betrouwbare, veilige en gegarandeerde levering van elektronische berichten. Bij OM worden de berichten, en daarmee het procesdossier, in haar infrastructuur ontvangen en doorgeleid naar en verwerkt in de GPS-applicatie. GPS is het processysteem waarmee het OM en de Rechtspraak grote delen van de werkprocessen mee ondersteunen.

4.2. Papieren overdracht

Bij de papieren overdracht wordt de dossiervormer van de politie ondersteunt met processystemen, zoals de applicatie(s) BVH en/of OPP. Ook vanuit DPD kan er worden geprint voor papieren overdracht aan OM, maar dat wordt enkel uitgevoerd in het geval de elektronisch overdracht niet werkt. Bijvoorbeeld wanneer er technische onderbrekingen zijn in de elektronische route naar het OM.

Als het onderzoek is afgerond, worden door de dossiervormer van de politie de relevante documenten uit het papieren onderzoeksdossier samengepakt en in het procesdossier ondergebracht. In het geval er een digitaal dossier is en deze elektronisch getekende stukken bevat, worden deze geprint en bij het papieren procesdossier opgenomen.

Omdat een elektronische handtekening na printen als 'papieren handtekening' zelf niet kan worden gevalideerd op integriteit en authenticiteit, voert de dossiervormer van de politie een controle uit op de geprinte elektronische stukken. Dit gebeurt om na te gaan of de digitale weergave overeenkomt met de weergave op het papier. Daartoe waarmerkt de dossiervormer de papieren afschriften als 'kopie conform het (digitaal) origineel'. Deze handeling (het voor kopie conform waarmerken) wordt doorgevoerd door te verklaren welke stukken voor kopie conform worden aangemerkt, zoals via een PV van Bevindingen of een Summier PV. Het voor kopie conform waarmerken wordt al toegepast bij omvangrijke onderzoeken. Daar blijft het originele papieren dossier achter bij de politie. Een digitale kopie-conform wordt aan het OM verstrekt, met daarbij nog enkel één papieren verklaring voorzien van een 'natte handtekening', waarin is opgenomen dat de daarbij behorende kopieën conform de originelen zijn. De Hoge Raad kent bijvoorbeeld aan een proces verbaal middels de kopie conform verklaring dezelfde waarde toe als het origineel, tevens in het licht van de bijzondere bewijswaarde als bedoeld in art. 344 lid 2 Sv. (zie ECLI:NL:PHR:2014:1725 en

ECLI:NL:HR:2014:2955). Bij het OM is intern het voor kopie conform waarmerken ook een gebruikelijke werkwijze (zie ECLI:NL:GHARN:2010:BL7606 en ECLI:NL:HR:2014:2955).

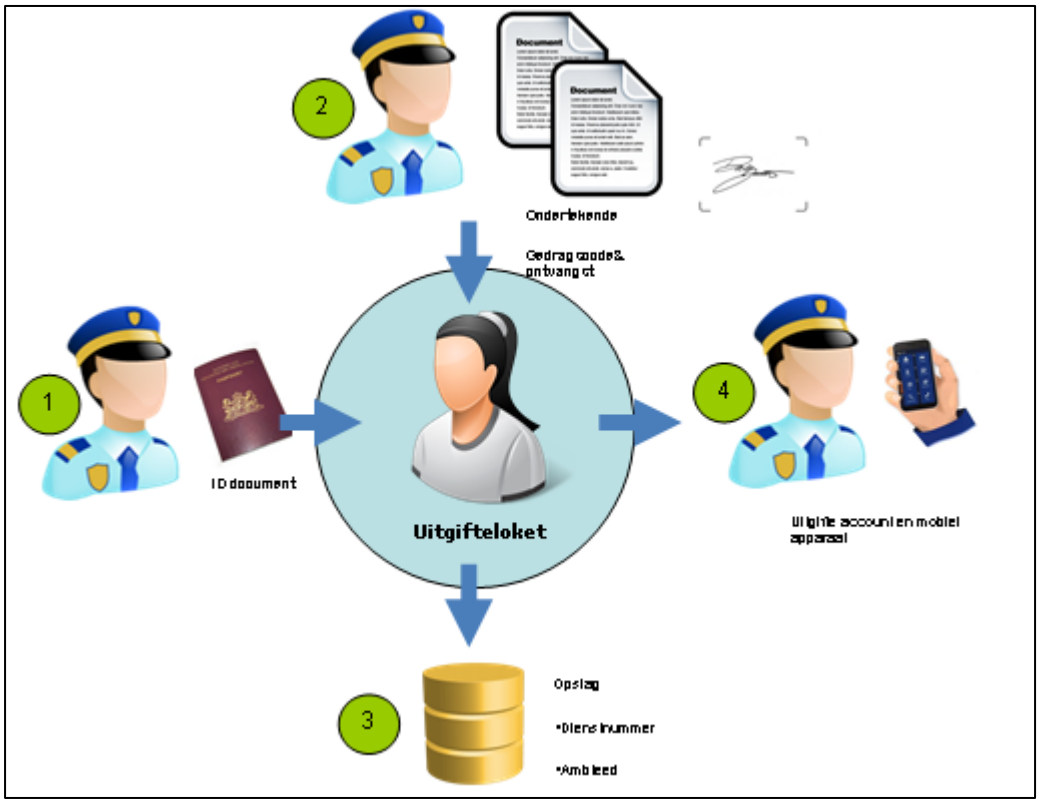
De dossiervormer controleert het dossier vervolgens op de gebruikelijke kwaliteitsaspecten en verstuurt volgens de gebruikelijke werkwijze het papieren dossier op naar het OM.

Het OM besteedt na ontvangst vervolgens het scannen van post/dossiers uit aan de Justitiële Informatiedienst (Justid). Daar word het papier procesdossier omgezet naar een digitaal procesdossier volgens een gecontroleerd proces (conform de procesvereisten aan die aan 'Vervanging' worden gesteld) en elektronisch teruggestuurd naar het OM. Dit versturen verloopt via het Elektronisch Berichtenverkeer (EBV), waarbij Justid gebruik maakt van een Axway, een infrastructuur voor betrouwbare, veilige en gegarandeerde levering van elektronische berichten. Bij het OM worden de berichten, en daarmee het procesdossier, na ontvangst verwerkt in de GPS-applicatie. GPS is het systeem waarmee het OM en de Rechtspraak grote delen van de werkprocessen mee ondersteunen.

Bijlage 1. **Uitgifteproces diensttelefoon**

Uitreiken van het mobiele apparaat
Het uitreiken van de politie diensttelefoon gebeurt binnen de politie op een geprotocolleerde wijze. Tijdens dit uitreiken ontvangt de verbalisant initieel zijn/haar autorisaties voor de politiesystemen die gekoppeld zijn aan zijn/haar functie/bevoegdheden. Bij beëindiging of verandering van functie wordt indien nodig de mobiele diensttelefoon ingenomen, en komen de autorisaties te vervallen of worden deze aangepast. De volgende stappen zijn bij het uitreiken te onderscheiden (Figuur 1: Uitgifteproces diensttelefoon):

- De verbalisant legitimeert zich met een wettelijk identificatie document (WID) bij een uitgifteloket. Het WID van de opsporingsambtenaar wordt vastgelegd en deze gegevens worden centraal opgeslagen.
- De verbalisant tekent voor ontvangst van de mobiele diensttelefoon en de daarvoor geldende gedragsregels voor het gebruik.
- Het uitgifteloket registreert het IMEI nummer (uniek nummer apparaat) en het diensttelefoonnummer en koppelt deze gegevens aan het account van de opsporingsambtenaar met het mobiele apparaat.
- De verbalisant activeert vervolgens (met zijn/haar persoonlijke codes) de mobiele diensttelefoon. Op de mobiele diensttelefoon krijgt de verbalisant geautoriseerde toegang tot de politieomgeving en de bijbehorende applicaties gebaseerd op zijn/haar rechten in de Active Directory (AD). Hierdoor is altijd bekend wie de applicatie gebruikt.



Figuur 1: Uitgifteproces diensttelefoon

De Active Directory (AD) is een beveiligd registratiesysteem waarin rechten worden geregistreerd. Alleen daartoe specifiek geautoriseerde medewerkers kunnen een verbalisant daarin toevoegen of verwijderen. In de AD wordt exact vastgelegd welke verbalisant op basis van zijn/haar functie welke rechten mag hebben op welke systemen en applicaties. Bij verwijdering heeft de medewerker geen mogelijkheid meer om gebruik te maken van systemen en applicaties. Door middel van bovenstaand punt 4 is gegarandeerd dat alleen deze verbalisant zijn eigen mobiele diensttelefoon kan gebruiken. Het is technisch niet mogelijk om met een andere gebruikersnaam op het betreffende apparaat in te loggen.

Vermissing of diefstal
De verbalisant moet bij vermissing of diefstal melding doen via de afgesproken procedures. Bij verlies of diefstal is het mogelijk om het mobiele apparaat door middel van plaatsbepaling op afstand te lokaliseren. Tevens kan het toestel op afstand worden gewist.

Defect of storing
Bij defect of storing moet de verbalisant zich melden bij de service desk. In geval van een storing wordt deze verholpen door de service desk. Bij een defect wordt het defecte apparaat gewist en vernietigd (shredder) en wordt een nieuw apparaat verstrekt door het uitgifte loket volgens het standaard protocol.

Bijlage 2. **Aanwijsbesluit authenticatiemiddel t.b.v. ondertekenen**

De politie ICT voorziening voor de elektronische handtekening (ondertekenvoorziening) en het in te zetten twee (of meer) factor authenticatiemiddel is conform het Besluit digitale stukken Strafvordering (art. 5 lid c) door de korpschef aangewezen als middel dat is ingericht om rechtsgeldig stukken te voorzien van elektronische ondertekening (zie: Figuur 2 en Figuur 3).

Besluit

Aanwijzingsbesluit middel voor elektronisch ondertekenen

Dit besluit heeft tot doel om een digitale voorziening als middel aan te wijzen die is ingericht om rechtsgeldig stukken te voorzien van elektronische ondertekening zoals bedoeld in de Wet digitale processtukken strafvordering en in de Algemene wet bestuursrecht en de eIDAS Verordening (EU) nr. 910/2014. Door hieraan te voldoen kan de "ondertekenvoorziening" worden ingezet in alle processen die Politie uitvoert.

Sinds 1 december 2016 is het Besluit digitale stukken Strafvordering van kracht. Dit besluit is een uitwerking van de Wet digitale processtukken strafvordering (2016). Deze wet maakt het mogelijk het gebruik van digitale processtukken te faciliteren en te kanaliseren. In de Wet digitale processtukken strafvordering staan wettelijke eisen ten aanzien van het waarmerken en tekenen van digitale documenten. In het nieuwe artikel 138e Sv is een omschrijving van een elektronische handtekening opgenomen. Hier wordt onder verstaan een handtekening die bestaat uit elektronische gegevens die gehecht zijn of logisch verbonden zijn met andere elektronische gegevens en die worden gebruikt door de ondertekenaar om te ondertekenen.

In het bestuursrecht is de elektronische handtekening al langer omschreven, maar als een open norm. Artikel 2:16 lid 1 van de Awb geeft aan dat aan de vereiste van ondertekening is voldaan door een elektronische handtekening, indien de methode die daarbij voor ondertekening is gebruikt, voldoende betrouwbaar is, gelet op de aard en inhoud van het elektronische bericht en het doel waarvoor het is gebruikt. Conform artikel 2:16 lid 2 moet er wel aan de eisen van de eIDAS Verordening (EU) nr. 910/2014 worden voldaan in die situaties waar er bij wettelijk voorschrift is bepaald dat een specifiek type elektronische handtekening als bedoeld in de Verordening wordt voorgeschreven. De voorziening voor elektronisch ondertekenen is dan ook zo ingericht dat tevens voldaan wordt aan de eisen van artikel 26 van de Verordening.

De kern van het in te zetten middel is gelegen in het gebruik van een speciaal door Politie ontwikkelde ondertekenvoorziening, bestaande uit een technische service en een Onderteken-app op de Politie smartphone. De Politie smartphone is door de Politie op persoon uitgegeven volgens een geprotocolleerd proces. De Onderteken-app op de smartphone ziet er op toe dat de authenticatie bestaat uit minimaal twee factoren. De technische service voorziet bij ondertekening in een onlosmakelijke verbinding van de unieke identiteit van de smartphone houder aan het exacte tekenmoment en het te tekenen document. Hierbij wordt een unieke hashwaarde berekent, welke controleerbaar maakt dat een elektronisch ondertekende tekst niet ongezien te wijzigen is (Cf. art 6 lid 1a / 2b Besluit en art 26 lid d Verordening). Zodra de

Figuur 2: Aanwijsbesluit middel voor elektronisch ondertekenen (pagina 1)


gebruiker in de Onderteken-app de ondertekening heeft bevestigd plaatst de ondertekenvoorziening een weergave van deze handeling in/op het (pdf)document:

Dit document is elektronisch ondertekend.

W.L.F. van der Kraats
inspecteur van Politie

Aldus vastgesteld te Den Haag

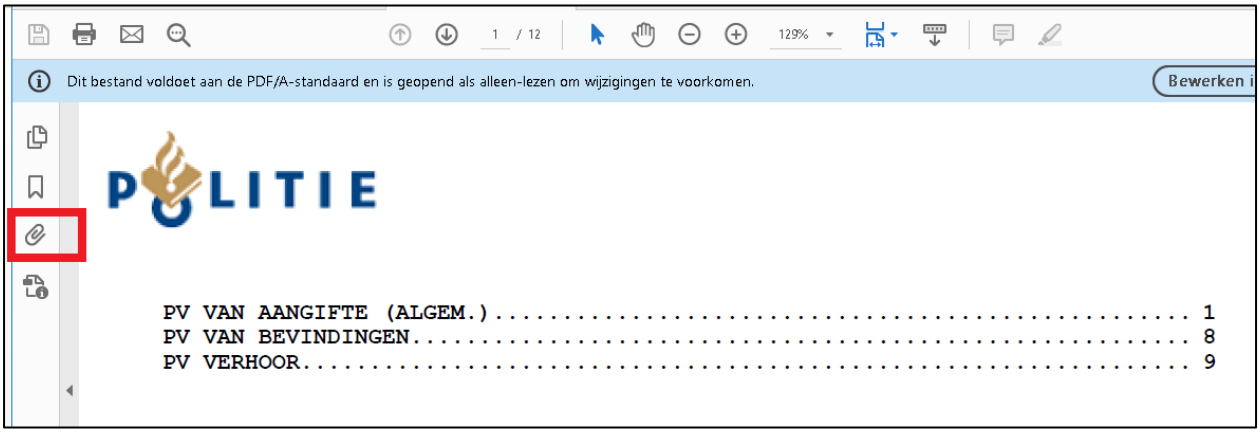
Figuur 3: Aanwijsbesluit middel voor elektronisch ondertekenen (pagina 2)

Bijlage 3. **Validatie**

Validatie van de authenticiteit en integriteit van een door de politiemedewerker elektronisch ondertekend document kan alleen met het digitale document. Indien een betrokkene papier onder ogen komt en twijfels heeft over de elektronisch handtekening of authenticiteit / integriteit van het document, kan men alsnog verzoeken het digitaal origineel verstrekt te krijgen. Dat kan door middel van een verzoek bij het OM / de zaaks OvJ. Het digitaal origineel kan gevalideerd worden op twee manieren.

PDF-documenten extraheren
Het kan voorkomen dat originele digitale stukken (pdf-documenten) als bijlage zijn toegevoegd in een overkoepelend digitaal procesdossier. In dergelijke gevallen moeten de originele stukken uit het procesdossier worden geëxtraheerd, zodat deze afzonderlijk kunnen worden gevalideerd. Deze extractie verloop als volgt:

1. Gebruiker klikt links op de paperclip in het geopende procesdossier (Figuur 4: Tonen van bijlagen via de paperclip).



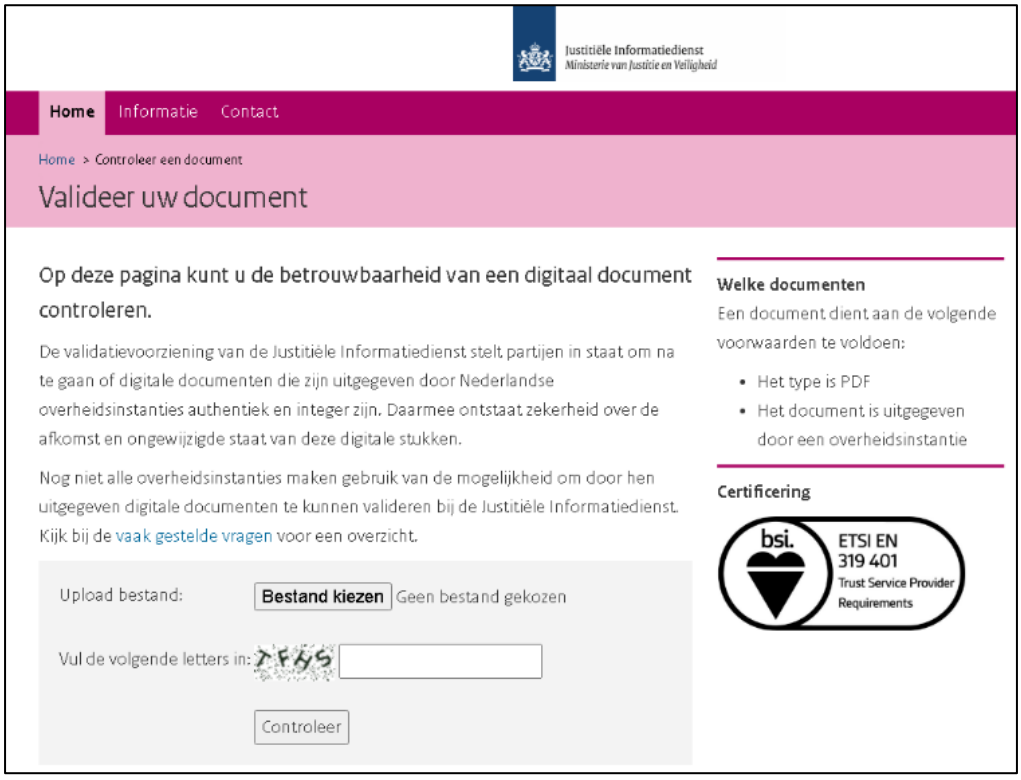
Figuur 4: Tonen van bijlagen via de paperclip

2. Links verschijnen de bijgevoegde brondocumenten. Met rechtermuisknop kunnen deze documenten worden via “Bijlage opslaan…” worden geëxtraheerd (Figuur 5: Extraheren van bijlagen).

Figuur 5: Extraheren van bijlagen

Validatie via GAAV

Navigeer in een webbrowser naar https://validatie.justid.nl, upload het digitaal ondertekende document door op "Bestand kiezen" te klikken en het bestand te selecteren. Vul de controleletters in en klik op controleer (zie: Figuur 6).



Figuur 6: GAAV portaal

Er zijn drie mogelijke uitkomsten: het document is authentiek en integer, het document is niet bekend of het document is bekend maar niet integer. Indien het document niet bekend is of niet integer, neem dan contact op met de instantie die het document heeft verstrekt.

1. Het document is *authentiek en integer*

2. Het document is *niet bekend*

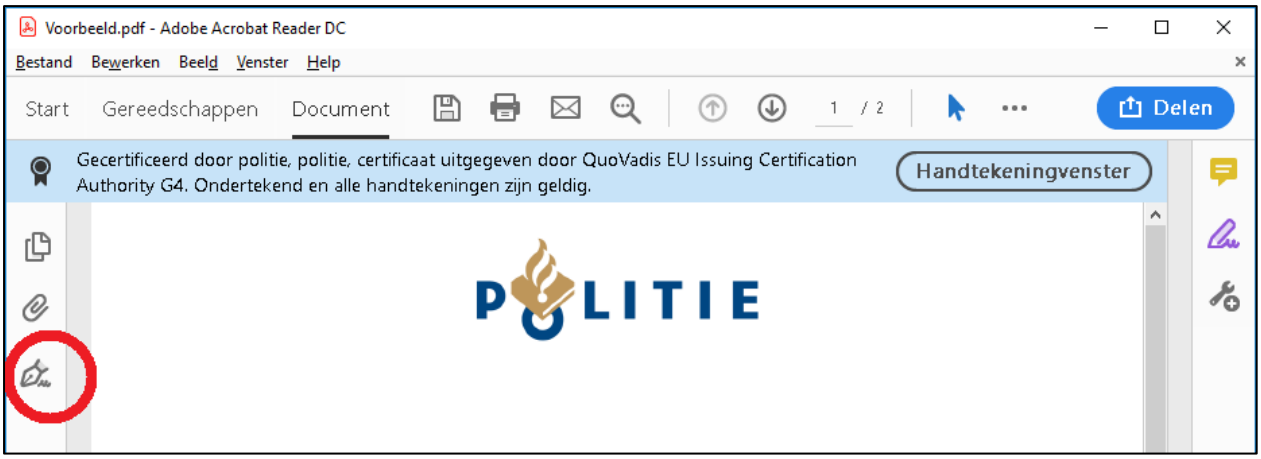
3. Het document is *bekend maar niet integer*

Validatie via Adobe Acrobat Reader

1. Open de het PDF-document pdf en ga na, of het een ongewijzigd politie-document is. In dat geval is een blauwe balk met certificeringsteken aanwezig, waarin de tekst weergeeft dat het document gecertificeerd is door de politie (Figuur 7: Certificeringskenmerk).

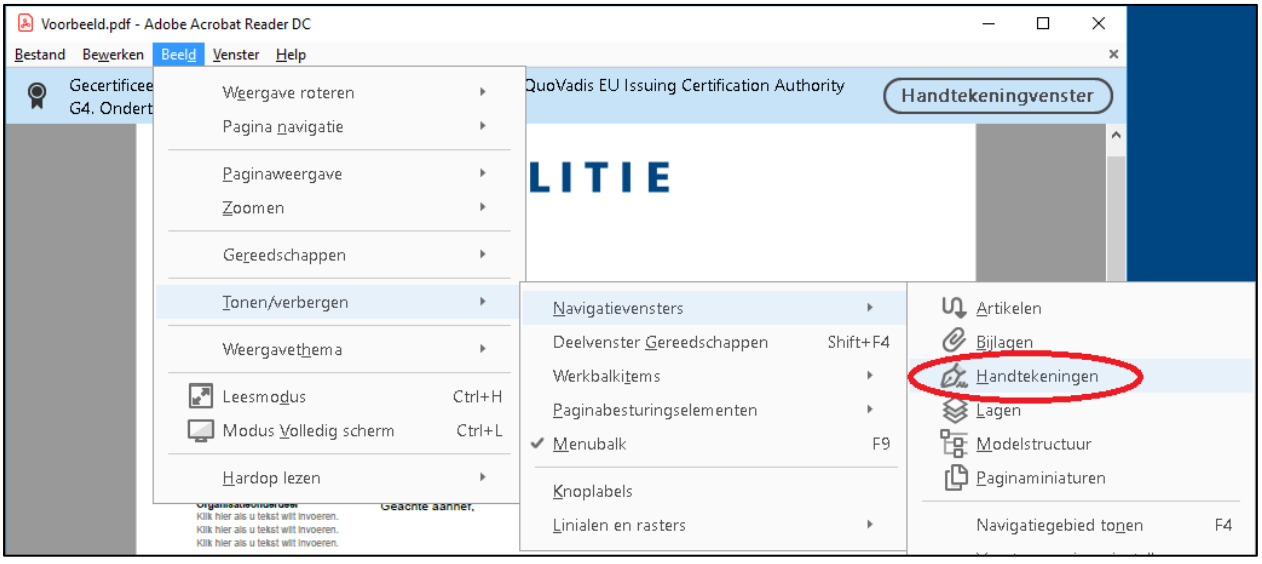
Figuur 7: Certificeringskenmerk

2. Klik op het handtekening-icoon (Figuur 8: Handtekening icoon).



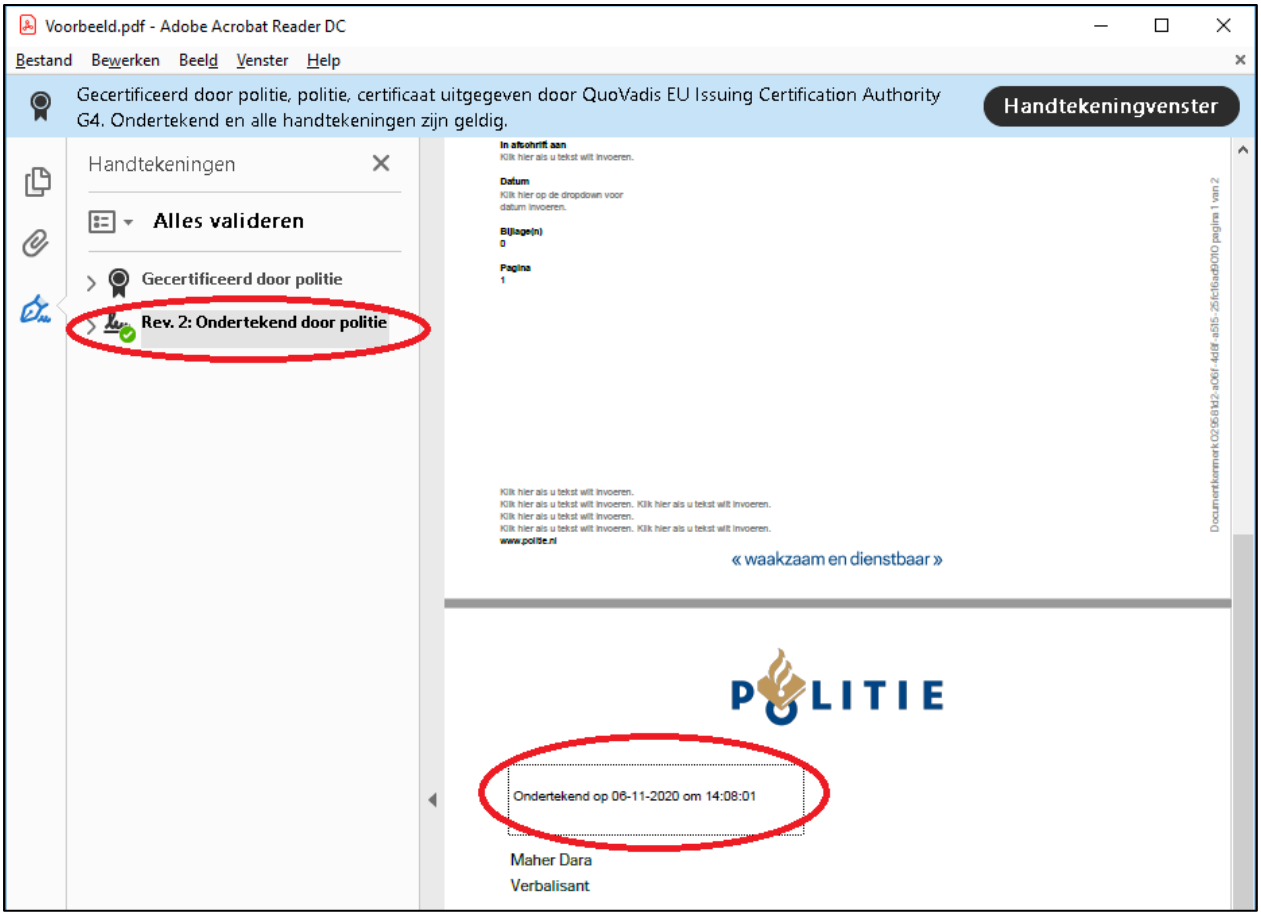
Figuur 8: Handtekening icoon

Als de handtekening icoon niet zichtbaar is kan deze ook worden getoond via de menubalk (Figuur 9: Handtekening icoon tonen).



Figuur 9: Handtekening icoon tonen

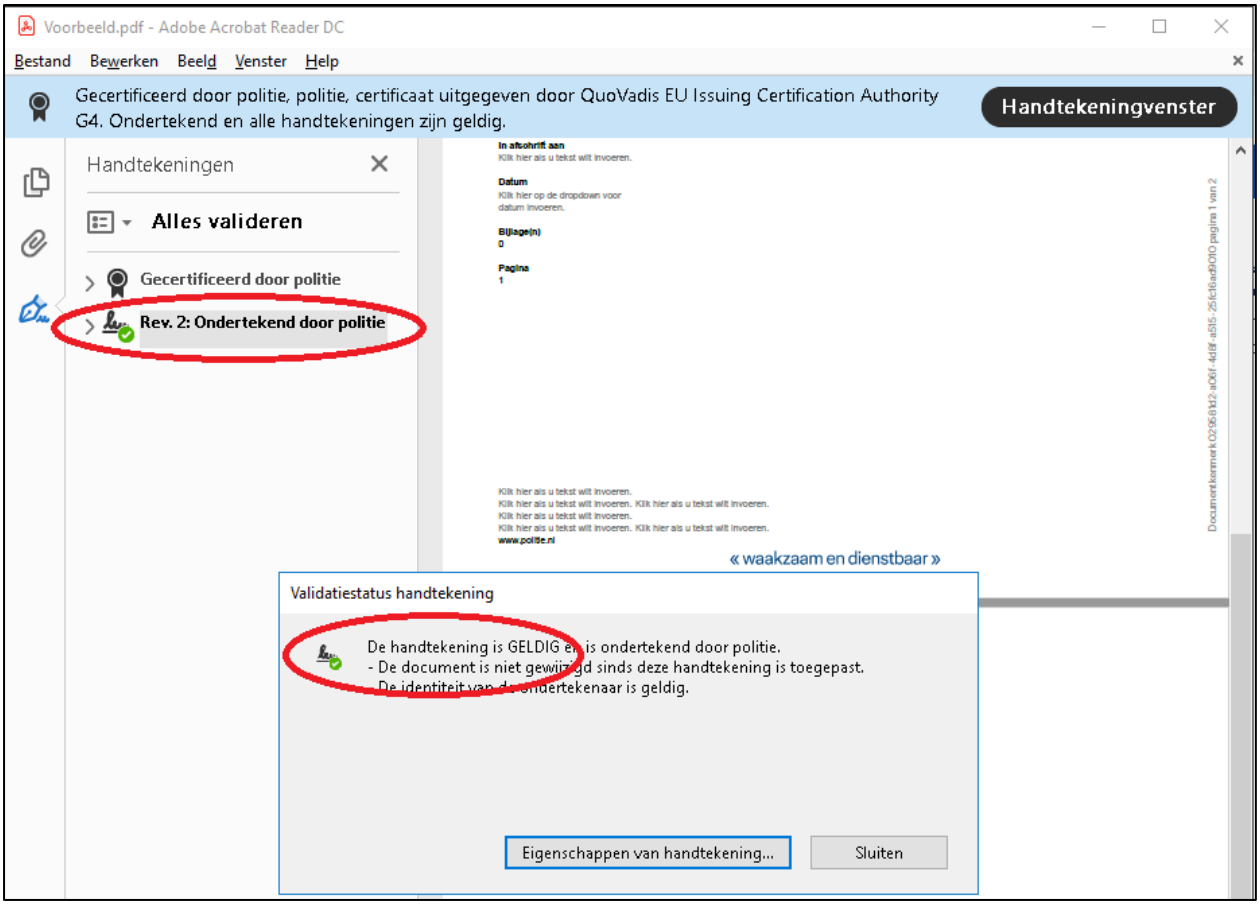
3. Het handtekeningen-venster komt tevoorschijn. Hierin zijn de handtekeningen van het PDF-document zichtbaar. Klik op een handtekeningregel: hierdoor navigeert Adobe Acrobat Reader naar het handtekeningveld (
Figuur 10: Handtekening **veld**).



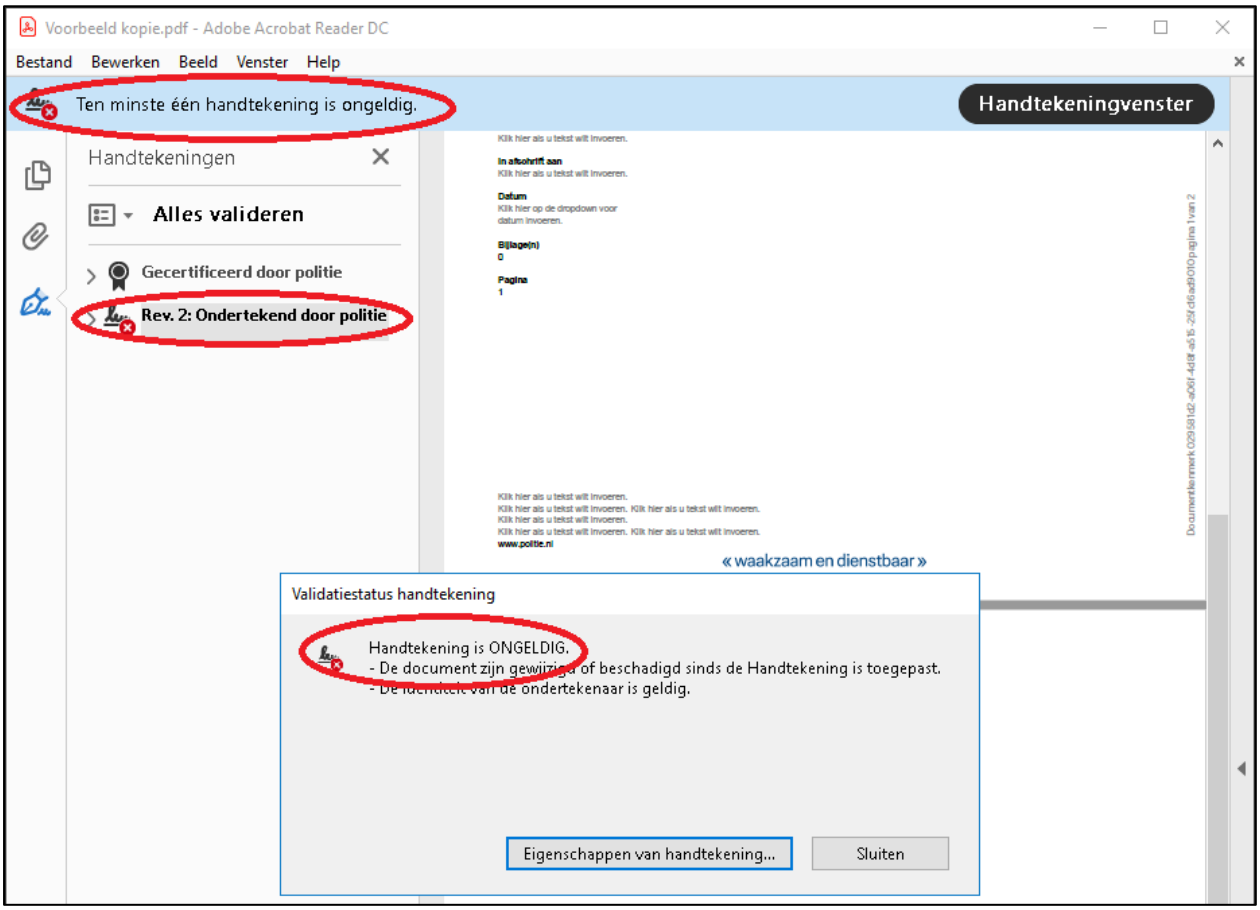
Figuur 10: Handtekening veld

4. Klik met linkermuisknop op de handtekeningtekst ("Elektronisch ondertekend op <datum>") in het document. In het venster "Validatiestatus handtekening" leest u of het certificaat geldig is. Dit betekent dat het document sinds de toepassing van het zegel (met daaronder het certificaat) niet is gewijzigd en dat de handtekening daarmee ook ongewijzigd is, aangezien die zich in het PDF-document bevindt. De handtekening bestaat daarbij onder andere uit de visuele kenmerken van de ondertekenhandeling (zoals dagtekening, ondertekenaar en rol) in het PDF-document. Deze gegevens zijn óók vastgelegd in het zegel. Het zegel zorgt er samen met enkele andere waarborgen voor dat de authenticiteit en integriteit van het document is geborgd en de geavanceerde elektronische handtekening voldoet aan wetgeving.

   PDF-viewers geven de controle van een certificaat op organisatieniveau (zoals bij de politie) momenteel ongelukkig weer. Er wordt gesproken over een 'ondertekening door politie' terwijl in feite alleen het beschermende certificaat (van het zegel) van de politie is en de ondertekening in het document door de geïdentificeerde en geautoriseerde ondertekenaar (zoals door de waarborgen afgedwongen). In een PDF-document met geldige elektronische handtekeningen wordt de geldigheid van de handtekening getoond wanneer de gebruiker op de handtekening klikt (zie: Figuur 11: Weergave geldige handtekening). In het geval dat het document en/of de handtekening wél is gewijzigd na ondertekenen, wordt hiervan een melding getoond (zie: Figuur 12: Weergave ongeldige handtekening). In Figuur 12 geeft de melding aan dat het document na ondertekenen is gewijzigd, maar dat het toegepaste certificaat onder het zegel geldig is. U dient een document waar een dergelijke melding optreedt niet te vertrouwen.

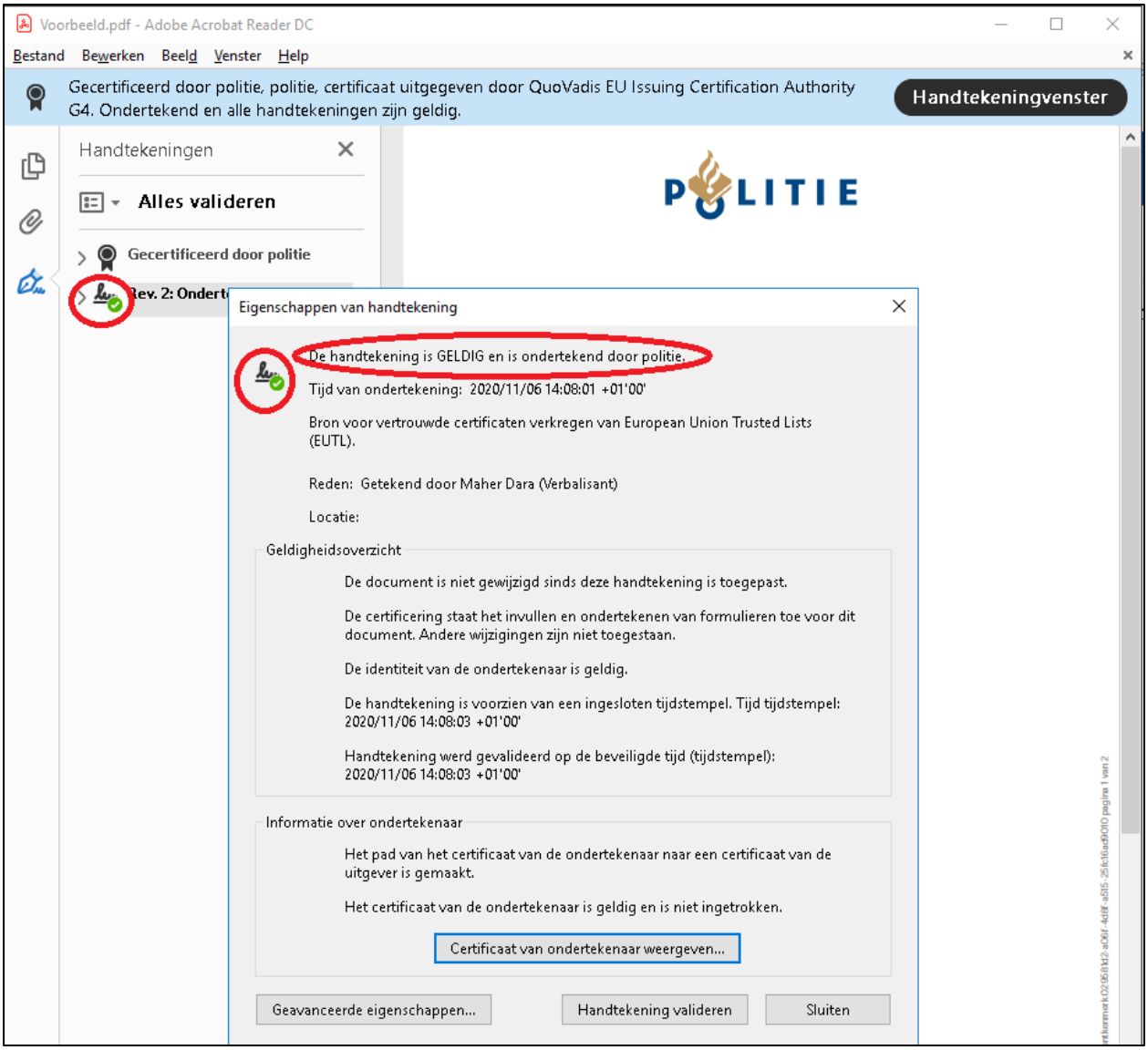


Figuur 11: Weergave geldige handtekening

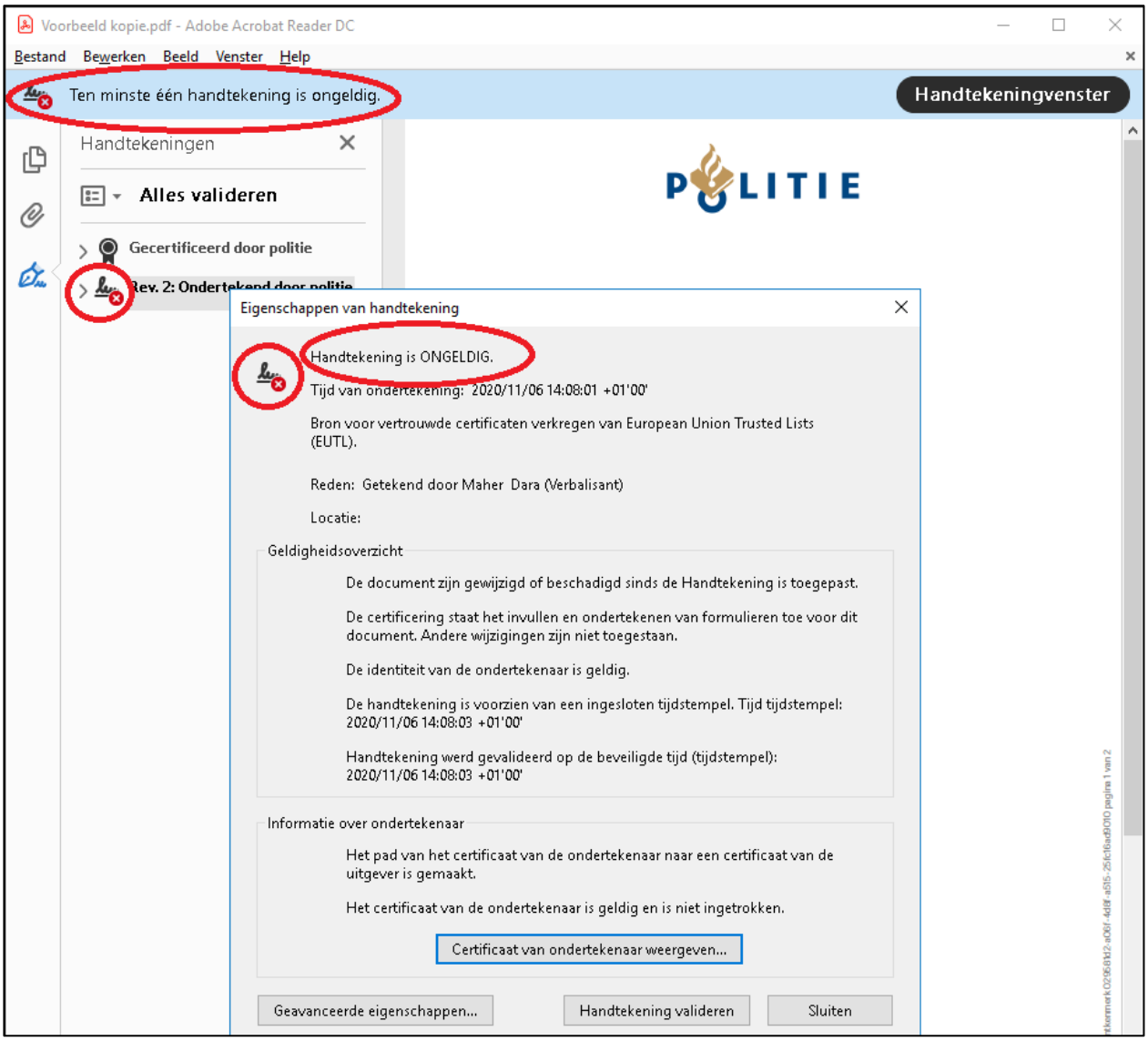


Figuur 12: Weergave ongeldige handtekening

5. Gebruiker kan meer details over de handtekening raadplegen door te klikken op de knop "*Eigenschappen van handtekening…*". Hier ziet gebruiker de gegevens over wie in welke hoedanigheid en op welk moment heeft getekend. Zoals ook het tijdstip van de ondertekening alsmede de naam van de ondertekenaar en zijn rol. Tevens ziet gebruiker nogmaals dat door de controle van het elektronische certificaat onder het zegel kan worden bevestigd dat het PDF-document (inclusief de handtekening) niet gewijzigd is. Omdat een PDF-viewer doorgaans het certificaat ongelukkig weergeeft, wordt de naam van de ondertekenaar weergegeven achter "*Reden:*". Daar ziet gebruiker door welke persoon het document is ondertekend en welke rol in het proces deze persoon had. Deze gegevens over de ondertekenaar worden geautomatiseerd geplaatst bij het ondertekenen en verzegelen; dit is één en dezelfde handeling. Dat betekent dat indien het certificaat geldig is en het document ongewijzigd, ook deze ondertekengegevens ongewijzigd en daarom betrouwbaar zijn. Op dit scherm is ook te lezen dat de beveiliging enkele handelingen op het document toestaat. Adobe Acrobat Reader verwoordt dit als volgt: "*De certificering staat het invullen en ondertekenen van formulieren toe voor dit document. Andere wijzigingen zijn niet toegestaan.*" Dit betekent dat indien het PDF-document een invulformulier zou hebben bevat, deze gevuld zou mogen worden. Het PDF-document bevat echter geen invulformulier. Tevens heeft de controle van de handtekening reeds aangetoond dat het document níet is gewijzigd sinds het zetten van de handtekening. Andere PDF-viewers verwoorden de toegestane wijzigingen nog onduidelijker, maar er is in ieder geval géén mogelijkheid tot het wijzigen van de gegevens in het document, inclusief de handtekening. In Figuur 13 worden eigenschappen van een geldige handtekening getoond en in Figuur 14 worden eigenschappen van een ongeldige handtekening getoond.



Figuur 13: Eigenschappen geldige handtekening

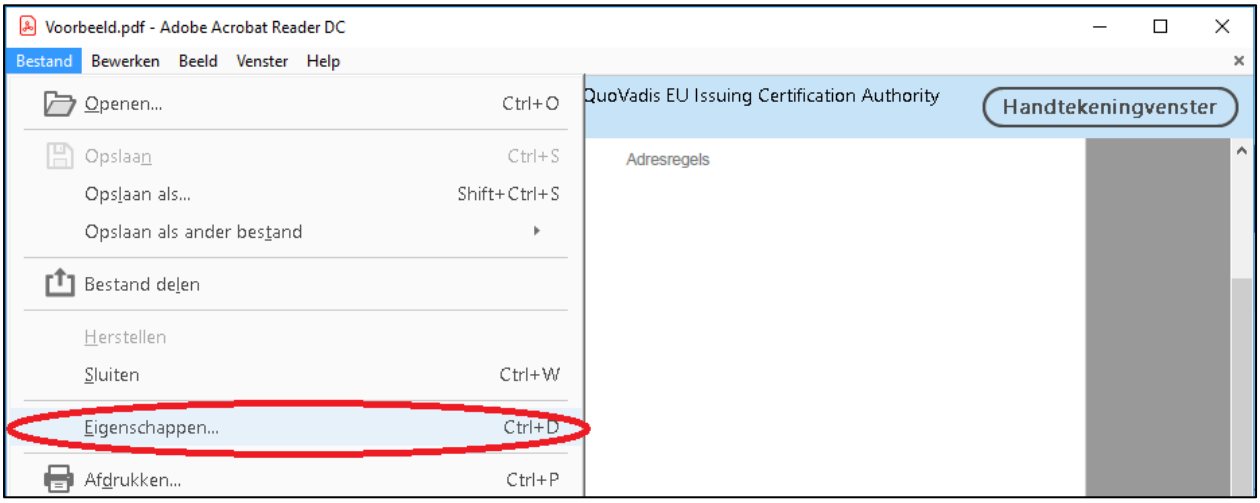


Figuur 14: Eigenschappen ongeldige handtekening

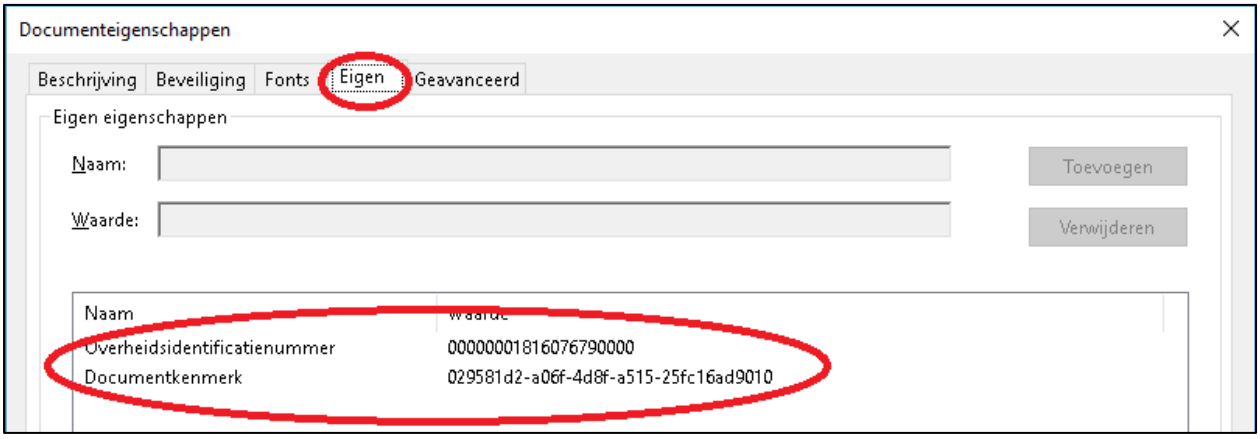
Bijlage 4. **Visuele kenmerken in / op het document**

Metadata in de pdf

1. Open het PDF-document en klik op Eigenschappen in het menubalk.



2. In het venster Documenteigenschappen zijn onder het tabblad '*eigen*' het *Overheidsidentificatienummer* van politie en het unieke *Documentkenmerk* zichtbaar.



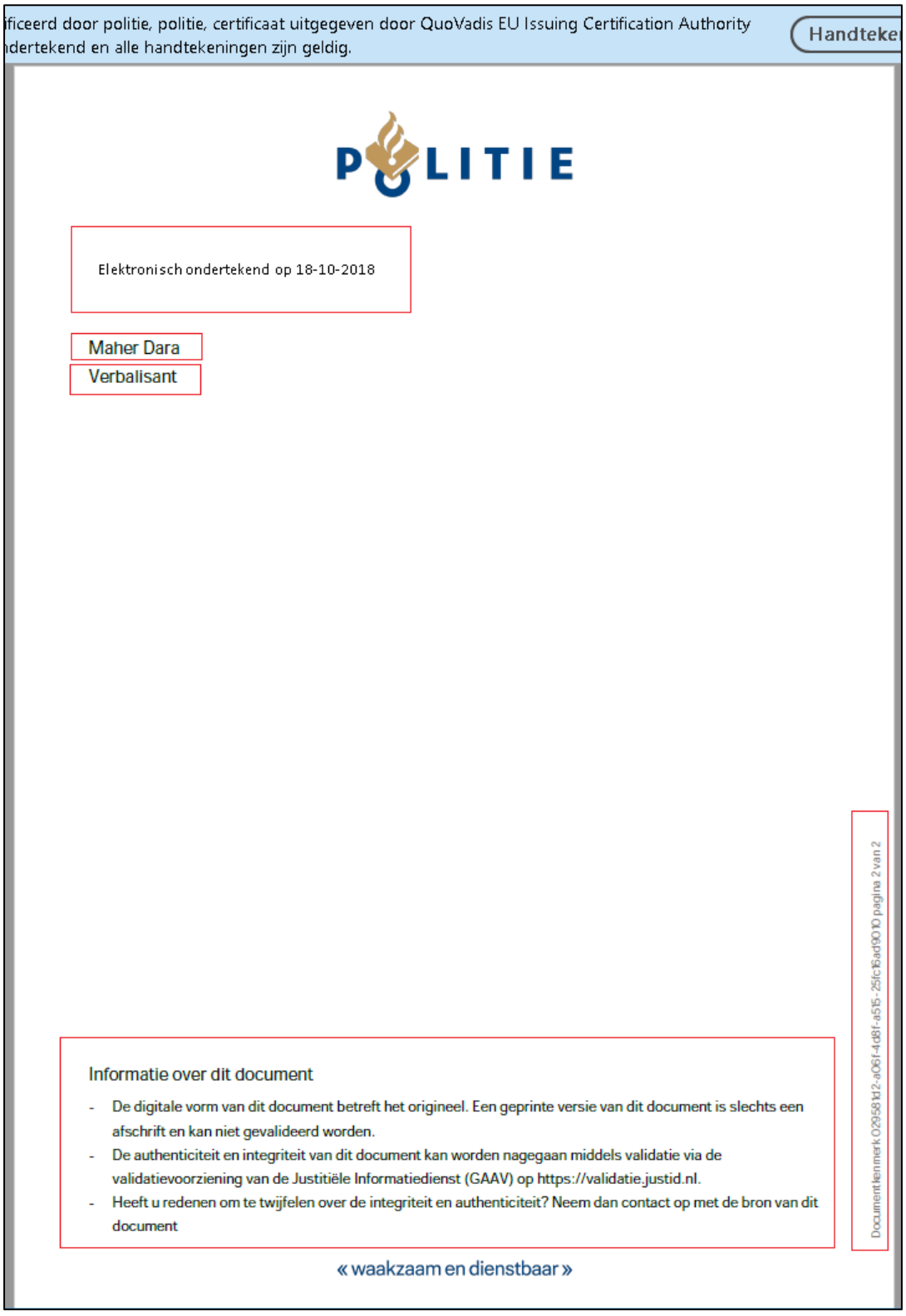
Weergave van de elektronische handtekening op het PDF-document

De politie geeft haar elektronische handtekening op twee manieren weer; op een tekenblad of in-line. De elektronische handtekening is in beide gevallen identiek en toont wie er getekend heeft, wanneer en in welke hoedanigheid / rol in het proces. In gangbare PDF-viewers is door te klikken op de handtekening-tekst om meer gegevens over de handtekening in te zien.

Tekenblad weergave (DPD)

Het tekenblad is de laatste pagina van een ondertekend document, waarop de elektronische handtekening(en) worden weergegeven. Het tekenblad bevat de volgende informatie ter ondersteuning van de correcte interpretatie van een digitaal ondertekend document, ook als deze geprint is:

- een disclaimer die uitleg geeft over het feit dat het document elektronisch is getekend, waar het te valideren is, en waar men terecht kan bij twijfel over de echtheid/compleetheid van het document en/of de handtekening(en);
- een uniek kenmerk, zodat een lezer hieraan kan refereren in de communicatie naar de politie: ik twijfel over de authenticiteit van document xyz, kunt u mij dat verstrekken?;
- paginanummering en het totaal aantal pagina's, zodat een lezer kan vaststellen of een papieren exemplaar volledig is; en
- de visuele weergave van een elektronische handtekening bevat de datum van ondertekening.



Inline weergave (OPP)

Bij de zogeheten inline weergave zijn de elektronische handtekening(en) verwerkt binnen de pagina's van het document; er is geen tekenblad. Het document bevat o.a.:

- een uniek kenmerk, zodat een lezer hieraan kan refereren in de communicatie met de politie: ik twijfel over de authenticiteit van document xyz, kunt u mij het originele document verstrekken?; en
- een visuele weergave van een elektronische handtekening, die tevens de datum ondertekening bevat.


PKIoverheid Organisatie Services CA - G3. Ondertekend en alle handtekeningen zijn geldig.

Documentkenmerk:
ad4c58-1b9e-44af-b0f4-65fd51018386

1: niet is gebleken dat betrokkene de nationaliteit heeft van een staat die geen medewerking verleent aan gedwongen terugkeer of waarvoor een vertrekmoratorium of een andere beleidsmatige belemmering voor de uitzetting geldt[1];
3: door betrokkene geen/onvoldoende verifeerbare gegevens zijn verstrekt ter onderbouwing van de (gestelde) identiteit en nationaliteit. Niet gebleken is dat het onmogelijk is om deze gegevens te verstrekken;
4: niet is gebleken dat het (mogelijke) land van herkomst geen (vervangende) reisdocumenten zal verstrekken voor gedwongen terugkeer.

De maatregel is opgelegd:

Plaats	: Den Haag
Datum	: 18/10/2018
Tijd	: 17:10 uur.

De Staatssecretaris van Justitie en Veiligheid,
namens deze,
de hulpofficier van justitie,

Elektronisch ondertekend op 18-10-2018

M. Dara
inspecteur van Politie

Bijlage 5. **Accreditatie verklaring certificaat leverancier**

digicert + QuoVadis

Memo

To : Politie
From : P. Beckman Lapré
Date : 26 augustus 2019
Subject : QuoVadis onder toezicht van de Nederlandse overheid

C.C. : R. Berentsen, P. Mosch, L. van der Palm
:

Politie neemt een ondertekenvoorziening in gebruik waarmee stukken digitaal kunnen worden ondertekend (waarmerkservice).

De ondertekenvoorziening van Politie maakt gebruik van een zogenaamd 'Public Key Infrastructure' (PKI) certificaat door middel van de ondertekensoftware van QuoVadis. QuoVadis is een Qualified Trust Service Provider (QTSP) onder de ETSI standaarden, geaccrediteerd door Agentschap Telecom in Nederland. QuoVadis staat hiermee onder toezicht van de Nederlandse overheid.

- De accreditaties van QuoVadis zijn terug te vinden op: QuoVadis-Accreditaties.
- Voor de actuele lijst met organisaties die in Nederland zijn geaccrediteerd als Trust Service Providers wordt door het Agentschap Telecom verwezen naar de Trusted List Browser.

De status van de accreditatie van QuoVadis kan te allen tijde worden ingezien op Trusted List Browser – QuoVadis.

P. Mosch
Director Finance & Administration

P. Beckman Lapré
Director Sales & Marketing

Bijlage 6. **Brochure Elektronisch ondertekenen in de strafrechtketen**

POLITIE

Elektronisch ondertekenen in de strafrechtketen

Digitalisering strafrechtketen

Dit dossier bevat elektronisch ondertekende stukken. Deze brochure duidt de wettelijke status van de elektronische handtekening, de gehanteerde waarborgen en hoe deze is te verifiëren.

Inleiding

Het verwerken van papieren processtukken door digitale stukken die elektronisch worden ondertekend, is een belangrijke verbetering in de strafrechtketen. De doelmatigheid en kwaliteit van het strafrechtproces worden zo verbeterd. Data hoeven niet meer overgetypt te worden, met minder kans op typefouten. Ook worden niet langer slecht leesbare kopieën van documenten of foto's aan een dossier toegevoegd.

Werken met digitale processtukken gaat via diverse voorzieningen voor:

- het elektronisch ondertekenen van stukken;
- het waarborgen van de integriteit van de processtukken (pdf, data of beeld/geluid);
- het indienen of verstrekken van processtukken; en
- het valideren van de authenticiteit van processtukken

Wetgeving

Per 1 december 2016 is het Besluit digitale stukken Strafvordering (het Besluit) van kracht. Dit Besluit is gebaseerd op de Wet digitale processtukken strafvordering. Deze wet heeft het mogelijk gemaakt het gebruik van digitale processtukken te faciliteren en te kanaliseren.

Drie regelingen in deze wet gaan in op de volgende aspecten:

(1) de integriteit van processtukken in elektronische vorm;
(2) het elektronisch tekenen van processtukken; en
(3) het langs elektronische weg doen van aangifte, indienen van verzoeken, schriften en klaagschriften, instellen van rechtsmiddelen en kennisnemen van processtukken.

De wijzigingen als gevolg van de **Wet herziening tenuitvoerlegging strafrechtelijke beslissingen**, maken bovendien de kennisgeving van gerechtelijke mededelingen langs elektronische weg mogelijk.

Met deze regelingen over het elektronische verkeer tussen de rechtstreeks belanghebbenden (zoals de verdachte of het slachtoffer) en de rechterlijke instanties wordt geborgd dat digitale stukken op de juiste wijze worden ingebracht in het strafproces. Naar verwachting zal de modernisering van het Wetboek van Strafvordering en voorts op de beoogde Innovatiewet Strafvordering op termijn het gebruik van multimedia (beeld en geluid) mogelijk maken. Aan de integriteit van de multimedia worden dezelfde eisen gesteld als aan de integriteit van de overige digitale processtukken.

Eisen en het gebruik van de elektronische handtekening

De Wet digitale processtukken strafvordering heeft tot wijzigingen geleid van het Wetboek van Strafvordering (Sv). Daarin zijn de wettelijke eisen ten aanzien van het waarmerken en tekenen van digitale documenten opgenomen. In artikel 138e Sv is een definitie van een elektronische handtekening opgenomen:

> **Onder een elektronische handtekening wordt verstaan een handtekening die bestaat uit elektronische gegevens die gehecht zijn aan of logisch verbonden zijn met andere elektronische gegevens en die worden gebruikt door de ondertekenaar om te ondertekenen.**

De eisen aan de elektronische handtekening zijn van toepassing op alle (proces)stukken waarvoor het Wetboek van Strafvordering een handtekening of de ondertekening voorschrijft.

Het Besluit gaat verder in op de eisen en het gebruik van de elektronische handtekening. Er zijn twee mogelijkheden om een digitaal document rechtsgeldig te ondertekenen:

1. **Verbalisant:**
   Het plaatsen van een *elektronische handtekening* op een digitaal document (als bedoeld in art. 6 lid 1 Besluit).
2. **Burger**
   Het gebruik van de *tablet-handtekening* voor het plaatsen van een handtekening op een document, onder toezicht van een opsporingsambtenaar (als bedoeld in art. 6 lid 2 Besluit).

Authenticatie en associatie

Het elektronisch ondertekenen (of waarmerken) van stukken is altijd een combinatie van twee processtappen, namelijk authenticatie en associatie.

Met **authenticatie** levert de ondertekenaar bewijs van zijn identiteit. Voor het elektronisch ondertekenen door ambtenaren van politie geldt dat zij zich moeten authentiseren met een middel dat voldoet aan (art. 5 Besluit):

- het middel is uitgegeven door de overheid, of een onder toezicht van de overheid staande organisatie;
- het middel gaat uit van een twee-factor-authenticatie of hoger; en
- het middel is aangewezen door de bevoegde instanties.

Met de **associatie** worden gegevens over de ondertekening onlosmakelijk verbonden met het document. De associatie dient te voldoen aan de volgende eisen (art. 6, lid 1b Besluit): *de gegevens waaruit de elektronische handtekening bestaat, zijn op zodanige wijze verbonden aan de elektronische gegevens waarop deze betrekking heeft, dat de identiteit van de ondertekenaar, het moment van ondertekening en elke wijziging na ondertekening van de gegevens kan worden vastgesteld.*

> **De eisen aan de elektronische handtekening gelden voor alle stukken waarbij het Wetboek van Strafvordering een handtekening of ondertekening voorschrijft.**

Met de ondertekening wordt niet alleen voldaan aan de wet, maar ondertekening heeft in de praktijk ook een verduidelijkende functie. Door het plaatsen van een handtekening (bewuste handeling) is niet alleen de ondertekenaar, maar ook de ontvanger van het document zich bewust van de betekenis van het rechtsgeldige document. Het document is het resultaat van een rechtsgeldige handeling.

De burger (aangever, verdachte of getuige) ondertekent ten overstaan van een bevoegd ambtenaar met een *tablethandtekening*. Voor deze handtekening-vorm is geen (tweefactor) authenticatie nodig als bedoeld in artikel 5 van het Besluit. Bij de tabletHandtekening wordt een handtekening aangebracht op een gevoelige plaat, zoals een smartphone of tablet. Na het plaatsen van deze handtekening kan de inhoud van het elektronische document niet meer worden gewijzigd. De elektronische handtekening die vervolgens wordt gezet door de bevoegde ambtenaar garandeert dat het document authentiek is.

De waarborgen

Het belangrijkste doel van het ondertekenen is de juridische acceptatie van het document. Bij het behandelen van de strafzaak op zitting mag er geen twijfel ontstaan over de integriteit en de onderteken

Versie 1.0
23-11-2020

Figuur 15: Brochure (pagina 1 en 2 van 4)

betrekking heeft is verbonden, dat zowel de identiteit van de ondertekenaar, het moment van ondertekening en elke wijziging na ondertekening van het document zijn vastgesteld.

De politie zet de diensttelefoon in als twee-factor authenticatiemiddel. Medewerkers krijgen deze via een geprotocolleerd proces op de persoon uitgereikt. Dit middel is op 19 december 2019 door de korpsleiding aangewezen als het authenticatiemiddel voor de elektronische handtekening.

Het ondertekenproces

De medewerkers van de politie hebben toegang tot vaste en mobiele werkplekken. Daarop inloggen verloopt altijd via de daartoe ingerichte veiligheidsmaatregelen. Daarna logt hij/zij in op een applicatie, maakt een document aan en zet het document klaar voor ondertekenen. Vervolgens klikt de gebruiker op de ondertekenknop in de procesapplicatie en zet daarmee een ondertekenverzoek door aan de *Ondertekenvoorziening* van de politie. De desbetreffende verbalisanten krijgen een tekenverzoek op hun mobiele telefoon. In de beveiligde ondertekken-app op de telefoon kunnen zij het document inzien, ondertekenen of weigeren.

Zodra de verbalisant heeft ondertekend, stuurt de app dit naar de Ondertekenvoorziening. Deze voorziening plaatst visuele kenmerken van de ondertekening in/op het (pdf)document en maakt het *associatierecord* als bewijsstuk van ondertekening aan. Vervolgens krijgt het processysteem het getekende document terug, waarna het proces verder kan.

Integriteitshashwaarde

Het is belangrijk om vast te stellen dat een elektronische handtekening in feite het 'vergrendelen' van een document is. Na ondertekening kan het niet meer onopgemerkt worden gewijzigd. Iedere tekst op een scherm is niets anders dan een rij enen en nullen in een bestand. Deze rij wordt door een *hash-algoritme* verwerkt tot een unieke uitkomst - een *'hashwaarde'* voor het desbetreffende getekende document. Een hashwaarde is bij het opnieuw berekenen over een gewijzigd document geheel anders dan voorheen. Daardoor is het document niet meer als authentiek of integer aan te merken. Iedere wijziging in een document na ondertekenen is controleerbaar (vgl. art. 149a lid 3 Sv van een processtuk in elektronische vorm kan de integriteit worden nagegaan).

De hashwaarde wordt vastgelegd in het associatierecord als bewijsstuk van ondertekening. Deze wordt op een beveiligde plaats opgeslagen. Een ontvanger van het elektronische getekende document kan de geldigheid van de ondertekening controleren ('valideren') op basis van een het digitale origineel en het Justitie validatieportaal (GAAV).

Papieren processtuk

In het geval men een papieren processtuk heeft ontvangen, voorzien van elektronische handtekening dient het dossier voorzien te zijn van een *kopie-conform verklaring*. Daarin staat aangegeven welke stukken gelijkgesteld zijn met het elektronisch getekende origineel. De kopie-conform verklaring wordt opgenomen in een proces-verbaal, voorzien van een natte handtekening. Papieren dossiers worden conform de huidige afspraken tussen de politie en het Openbaar Ministerie verzonden aan het pakket, waar het in de zogeheten de Justid-scanstraten onder het traject 'Verarging' (gecontroleerd proces) gedigitaliseerd wordt.

Het digitale origineel van elektronische getekende documenten is op te vragen bij het Openbaar Ministerie.

Validatieprocese lektronisch getekende stukken

Validatie van de handtekening is één van waarborgen onder de handtekening. Artikel 149a lid 3 Sv gaat hier op in: *van een processtuk in elektronische vorm kan de integriteit worden nagegaan doordat iedere wijziging daarvan kan worden vastgesteld*. Dit is uitgewerkt in art. 6, eerste lid van het Besluit. De wetgever doelt op controleerbaarheid en sluit zich daarbij voor dat dit langs elektronische weg zal plaatsvinden.

Het nagaan van de integriteit en authenticiteit, kortweg valideren, kan op verschillende manieren.

Zo kan het Justitie-validatieportaal worden gebruikt: *https://validatie.justid.nl*. Een andere manier is om in een PDF-viewer te klikken op de handtekening-tekst. Bij verdere twijfel kan men contact op nemen met de politie. De diverse manieren van valideren staan nader beschreven in het kader over 'Validatie in de praktijk.'

Audit

Omdat er voor de ondertekening eigen middelen en voorzieningen van de politie worden ingezet, dienen deze te worden geauditeerd. Dit is één van de eisen van het eerder genoemde Besluit. Onderscheiden worden een initiële audit en daarna periodieke audits.

Audits zijn van belang voor het vertrouwen in de elektronische handtekeningen en dienen als kwaliteitsbron. Een elektronische handtekening is immers slechts een set aan afspraken en waarborgen waaraan iedereen vertrouwen moet kunnen ontlenen en die iedereen moet kunnen controleren. De audits dienen uitgevoerd te worden door een onafhankelijke deskundige, die over de juiste onderzoeksmiddelen beschikken en beproefde onderzoeksmethoden toepassen.

Validatie in de praktijk

Het nagaan van de integriteit en authenticiteit, kortweg valideren, kan op verschillende manieren. Allereerst met behulp van de GAAV-validatiedienst van de justitiële informatiedienst (Justid): https://validatie.justid.nl . Justid is een zogeheten vertrouwensdienst (Trusted Service Provider) en is er op ingericht onafhankelijk, op basis van associatie records van ondertekeningen, een validatiedienst te leveren. In het validatieportaal kan men een document aanbieden ter validatie en krijt daarvan een validatie rapport.

Een andere manier van valideren kan via de gegevens over de ondertekening, zoals vastgelegd in het PDF-document tijdens het toepassen van het gekwalificeerde zegel van de politie. Gangbare PDF-viewers ondersteunen dit valideren van zegels (een actuele bijgewerkte PDF-viewer, zoals Adobe Reader, is wel een vereiste). Voor details over de ondertekening kan men klikken met de linkermuisknop op de weergave van de handtekening. Op dit scherm leest de gebruiker of de controle van het certificaat behorende bij het zegel geldig is. Dit betekent dat het document sinds de toepassing van het zegel niet is gewijzigd en dat de gegevens over de ondertekening daarmee ook ongewijzigd zijn. De handtekening bestaat daarbij onder andere uit de visuele kenmerken van de ondertekenhandeling (zoals dagtekening, ondertekenaar en rol) in het PDF-document. Deze gegevens zijn óók vastgelegd bij toepassing van het zegel.

PDF-viewers geven bij de controle van het politiezegel vaak 'ondertekening door politie' weer, terwijl deze ook wordt toegepast bij iedere ondertekening. De politie ziet toe op het verweken van de gegevens van de ondertekening.

Door in bijvoorbeeld Acrobat Reader op "Eigenschappen van handtekening..." te klikken worden de gegevens over de ondertekening getoond, namelijk: het tijdstip van de ondertekening, de naam van de ondertekenaar en zijn rol. Tevens ziet de gebruiker nogmaals dat door de controle van het certificaat onder het zegel kan worden bevestigd dat het PDF-document (inclusief de gegevens over de ondertekening) niet gewijzigd is.

Gecertificeerd door politie.

Daarnaast kan men bij verdere twijfels een validatie laten uitvoeren door contact met de verstrekker van het document, of met politie, zoals via de op het document vermelde eenheid en contactpersoon. De hashwaarde van het door de gebruiker ontvangen document wordt dan vergeleken met de hashwaarde die is opgeslagen in het associatie record.

« waakzaam en dienstbaar »

Versie 1.0
23-11-2020

« waakzaam en dienstbaar »

Versie 1.0
23-11-2020

Figuur 16: Brochure (pagina 3 en 4 van 4)