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 vervangen 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, schrifturen 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 voordien 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 procestukken.

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 proces-stappen, 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 waar 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 ondertekening van de digitale procestukken. Een document mag na ondertekening niet meer gewijzigd zijn. Ook moet duidelijk zijn wie het document heeft ondertekend. Daarom worden in en op grond van het Wetboek van Strafvordering (Sv) eisen gesteld aan de authenticatie van de ondertekenaar en de associatie van de handtekening met het document. Voor de ontvanger moet duidelijk zijn dat het document in overeenstemming met deze wet ondertekend is. Van de ondertekenaar zijn naam en hoedanigheid van de functionaris vermeld. De elektronische handtekening op zichzelf is niet zichtbaar; daarom wordt vermeld dat het processtuk elektronisch ondertekend is. De elektronische handtekening kan met behulp van validatie worden aangetoond.

Twee-factor authenticatie

Het authenticatiemiddel dient beschermd te zijn tegen onbevoegd gebruik, zodat de bevoegde instanties er zeker van kunnen zijn dat de persoon die zich met het middel identificeert, de exclusieve beschikking heeft over het middel. Dat kan door twee-factor-authenticatie, waarbij twee van de drie factoren gebruikt moeten worden: kennis (weten), bezit (hebben), zijn (vingerafdruk, oogscan). De factoren moeten een onderdeel zijn van het proces van ondertekening (de authenticatie), maar hoeven niet in tijd samen te vallen. Dit betekent dat het bewijs dat een opsporingsambtenaar levert van zijn identiteit bij inloggen op smartphone en/of bedrijfsprocessysteem kan worden hergebruikt tijdens ondertekenen. De identificerende attributen dienen tijdens ondertekenen te resulteren in een elektronische handtekening die op een zodanige wijze aan het elektronisch bestand waarop zij

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 december2019 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 onderteken-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.

Integriteit-hashwaarde

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 parket, waar het in de zogeheten de Justid-scanstraten onder het traject 'Vervanging' (gecontroleerd proces) gedigitaliseerd wordt.

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

Validatieproces elektronisch 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 stelt 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 kwaliteitsborg. 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

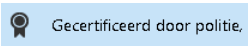
Het nagaan van de integriteit en authenticiteit, kortweg valideren, kan op verschillende manieren. Allereerst met behulp van de GAAV-validatiedienst van de justitiële informatiedienst (Justid): https://validatie.justid.nl . Justid is een zogeheten vertrouwensdienst (Trusted Service Provider) en is er 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 met het document verbonden 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 ondertekenvoorziening van 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.



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.

.