Interpretatie en controle elektronische handtekeningen die op een niet-persoonsgebonden certificaat gebaseerd zijn

Dit is momenteel (december 2024) de meest gebruikelijke methode van het elektronisch ondertekenen van documenten. Ondertekendienstverleners (zoals DocuSign, Evidos, Zynyo, Ondertekenen.nl, Signrequest, PKISigning, CM.com, Stiply, Signhost, etcetera) voorzien documenten van een elektronische handtekening op verzoek van hun klanten. Daarbij gebruik makend van een certificaat dat niet op naam van de ondertekenaar staat, maar veelal op naam van de ondertekendienstverlener.

Doordat het gebruikte certificaat voor de elektronische handtekening niet op naam van de ondertekenaar staat, kunt u de identiteit van de ondertekenaar niet afleiden uit de feitelijke elektronische handtekening die op het document staat. In de praktijk leveren ondertekendienstverleners veelal een tweede document (vaak een 'transactiebon', 'signing log' of vergelijkbaar genaamd) met daarop identificerende gegevens van de ondertekenaar(s). Het is van belang dat u begrijpt op welke manier de ondertekendienstverlener de identiteit van de ondertekenaar heeft vastgesteld.

Enkele veel gebruikte methodes zijn:

- Verificatie van de identiteit via e-mail. Bij deze methode wordt door de ondertekendienstverlener een code verstuurd naar het opgegeven e-mailadres. De ondertekenaar moet die code vervolgens invoeren om het document elektronisch te kunnen ondertekenen. Op deze wijze stelt de ondertekendienstverlener vast dat de ondertekenaar toegang heeft tot het opgegeven e-mailadres (en daarmee de identiteit van de ondertekenaar). Hoewel deze vorm van controle het bemoeilijkt om 'zomaar' een elektronische handtekening te kunnen plaatsen, is deze methode niet waterdicht.
    - Wanneer de code voor ondertekening bijvoorbeeld naar een algemeen e-mailadres verstuurd is (bijvoorbeeld info@ …), dan hebben in de praktijk vaak meerdere personen toegang tot dat e-mailadres. De identiteit van de ondertekenaar kunt u dan niet met zekerheid vaststellen.
    - Wanneer de code voor ondertekening naar een persoonlijk e-mailadres verstuurd is, dan is de kans op misbruik waarschijnlijk kleiner dan via een algemeen e-mailadres. Maar ook wanneer een persoonlijk e-mailadres wordt gebruikt, bestaat het risico dat iemand anders dan de beoogde ondertekenaar toegang tot de code krijgt. Dat zou kunnen doordat de computer van de ondertekenaar niet met een wachtwoord vergrendeld is. Maar daarnaast wordt niet alle e-mail beveiligd verstuurd, waardoor de code via Internet onderschept kan zijn.
      Uiteraard is het in deze situatie van belang dat u vaststelt dat het gebruikte e-mailadres daadwerkelijk het e-mailadres van uw cliënt is en uw cliënt daadwerkelijk zelf de code ingevoerd heeft om te ondertekenen.
- Verificatie van de identiteit via SMS. Bij deze methode stuurt de ondertekendienstverlener de code die nodig is om de elektronische handtekening te plaatsen via een sms-bericht naar een van tevoren opgegeven telefoonnummer. Dit betekent sowieso dat u zich ervan moet vergewissen dat het gebruikte telefoonnummer inderdaad het telefoonnummer van de ondertekenaar is en dat die telefoon door niemand anders gebruikt kan worden. Daarnaast zijn er telefoons waarbij de inhoud van sms-berichten op het startscherm getoond wordt, zonder dat de telefoon ontgrendeld hoeft te worden. In die gevallen kan iedereen die het scherm van de telefoon kan zien, de code voor ondertekening achterhalen. Bovendien moet stilgestaan worden bij huiselijke situaties, waarin partners toegang hebben tot elkaars telefoon en zodoende de beschikking over de code kunnen krijgen.
- Verificatie van de identiteit via iDIN. Bij deze methode moet de ondertekenaar inloggen in zijn/haar online bankieren-omgeving, om de elektronische handtekening te kunnen plaatsen. Bij deze vorm van identificatie leunt u dus sterk op het identificatiemechanisme van de desbetreffende bank. Hoewel het inloggen in een online bankomgeving doorgaans als veilig wordt beschouwd, moet u ook hier stilstaan bij huiselijke situaties of situaties waarin personen door anderen verzorgd worden en derden soms toegang tot de bankrekening hebben via het inlogmiddel van uw cliënt. Ook deze vorm van identificatie is niet waterdicht.

Controleer bij elektronische handtekeningen die gebaseerd zijn op niet-persoonsgebonden certificaten daarom altijd zorgvuldig welke methode van identificatie toegepast is, welke identificerende gegevens u ziet en of die combinatie voldoende betrouwbaar en passend is voor het doel waarvoor de handtekening is gezet. Trek voor uzelf ook steeds de parallel met handgeschreven handtekeningen om een afweging te maken of de identificerende gegevens uit dergelijke elektronische handtekening zich kunnen meten met de eisen die u voor hetzelfde doel zou stellen aan een handgeschreven handtekening.

Omdat de identificerende gegevens bij dit type handtekening meestal op een specifiek document staan (veelal de 'transactiebon', 'signing log' of vergelijkbaar aangeduid), dat meegeleverd wordt met het ondertekende document, moet u zorgvuldig vaststellen of beide documenten bij elkaar horen. Veelal wordt een uniek kenmerk op zowel het ondertekende document als op het document met de identificerende gegevens getoond, waarmee door de ondertekendienstverlener aangeduid wordt dat die documenten bij elkaar horen. Controleer dus goed of beide documenten betrekking hebben op dezelfde elektronische handtekening.

U zult hebben opgemerkt dat de ondertekendienstverlener een vrij prominente rol heeft in het identificatieproces van de ondertekenaar(s) en het verbinden van het document met de identificerende gegevens aan het ondertekende document. In algemene zin zullen dergelijke partijen als professionele dienstverleners acteren en hun dienstverlening zo zorgvuldig mogelijk in de markt zetten. Het is echter goed u ervan bewust te zijn wat de rol van dergelijke derde partijen is en dat daar potentieel fouten gemaakt kunnen worden.

Doordat voor de ondertekening van het document gebruik is gemaakt van een certificaat, kunt u exact controleren of het document na ondertekening al dan niet gewijzigd is. Wanneer u het ondertekende document in uw PDF-viewer opent en het handtekeningen scherm opvraagt, dan wordt daar vermeld of het document sinds ondertekening al dan niet gewijzigd is. Op het moment van publiceren van deze notitie zijn er geen gevallen bekend waarbij na ondertekening niet-detecteerbare wijzigingen zijn aangebracht. Wanneer uit deze controle blijkt dat het document na ondertekening niet gewijzigd is, dan kunt u daar dus met een hoge mate van zekerheid vanuit gaan.

Veel ondertekendienstverleners zetten hun eigen elektronische handtekening op het document met de identificerende gegevens van de ondertekenaar. Dat doen zij om controleerbaar te maken dat die informatie daadwerkelijk van hen afkomstig is op het moment van ondertekening en dat het document met identificerende gegevens na ondertekening niet gewijzigd is. Controleer daarom ook altijd de elektronische handtekening op dat document op de volgende punten:

- De naam waarop het gebruikte niet-persoonsgebonden certificaat staat: die zou op naam van de ondertekendienstverlener moeten staan;
- Of het tijdstip waarop het document met identificerende gegevens ondertekend is correspondeert met het tijdstip van ondertekening van het document dat uw client ondertekend heeft;
- Of het document met identificerende gegevens na ondertekening niet gewijzigd is, via het handtekeningenscherm in uw pdf-viewer.

Deze informatie hoort bij het thema Elektronische handtekening op knb.nl.

KNB, december 2024