

Digitale handtekeningen voor formulier-akkoorden

Voor: de VCA-tool (medewerker klikt in een web-app op "akkoord" voor personeelsreglement, veiligheidsvoorschriften, PMO-keuze).

Vraag: hoe maken we dat juridisch houdbaar?

Kort antwoord (voor wie weinig tijd heeft)

- **Ja, een klik op "akkoord" is juridisch geldig** in Nederland. Ook zonder dure tool.
 - Voor **interne** HR- en veiligheidsdocumenten is de **lichtste vorm (een klik met goede vastlegging)** genoeg.
 - De zwakte zit niet in de geldigheid, maar in het **bewijs** als een medewerker het later ontkent.
 - **Jullie zijn goed bezig:** wie/wanneer/wat + een SHA256-controlegetal is precies de goede basis.
 - **Drie verbeteringen** maken het sterk: (1) akkoord vastklikken **achter de persoonlijke login**, (2) een **gratis onafhankelijk tijdstempel** op het controlegetal, (3) de mailbevestiging met een **klik-link of code** in plaats van "reply".
 - Zwaardere handtekeningen (AES/QES via een betaalde tool) hou je achter de hand voor **echte contracten** (arbeidsovereenkomst, vaststellingsovereenkomst), niet voor toolbox-akkoorden.
-

1. Het juridische kader (eIDAS + Nederlands recht)

De Europese wet **eIDAS** kent drie niveaus van elektronische handtekening:

- **SES — simpele handtekening.** Een aangevinkt vakje of een "akkoord"-knop valt hier expliciet onder. Geen technische eisen. Geldig, maar het makkelijkst te betwisten.
- **AES — geavanceerd.** Uniek gekoppeld aan de persoon, identificeert die persoon, en wijziging van het document is achteraf detecteerbaar.

- **QES — gekwalificeerd.** Een AES met een officieel certificaat van een erkende partij + identiteitscontrole. **Wettelijk gelijk aan een handgeschreven handtekening in de hele EU.** Bij betwisting moet de tégenpartij bewijzen dat het niet klopt.

Nederlands recht (art. 3:15a BW): een elektronische handtekening heeft dezelfde rechtsgevolgen als een handgeschreven handtekening *"indien de methode die daarbij is gebruikt voor authenticatie voldoende betrouwbaar is, gelet op het doel..."*. Een rechter mag een handtekening dus **niet weigeren enkel omdat hij elektronisch is** (eIDAS art. 25). Hij weegt per geval: past de betrouwbaarheid bij het belang van het document?

Wat betekent dat voor jullie documenten?

- Personeelsreglement, veiligheidsinstructies, VCA-toolbox, PMO-keuze = **laag juridisch/financieel risico** (kennisname en instemming met interne regels).
- Daarvoor is een **goed vastgelegde klik (SES) juridisch voldoende**. Dit is geen expliciete wetsregel voor dit documenttype, maar volgt uit de open norm: laag risico → licht niveau mag.
- **Zwaarder (AES/QES) wil je pas** bij documenten met grote gevolgen: de arbeidsovereenkomst zelf, een vaststellingsovereenkomst (ontslag), of iets met grote financiële/juridische impact.

2. Het echte risico: bewijs bij betwisting

Bij een gewone klik-akkoord ligt de **bewijslast bij de werkgever** als de medewerker zegt "dat heb ik nooit geklikt". Jij moet dan aantonen dat déze persoon het écht deed.

Waarschuwend praktijkvoorbeeld — Hof Arnhem-Leeuwarden, 21 oktober 2025: een digitale handtekening (via een professionele tool) werd tóch **onvoldoende betrouwbaar** geacht, omdat het bedrijf niet kon aantonen h^oe de teken-link was verstuurd en dat déze persoon hem echt had geopend en getekend. De handtekening stond er wel, maar het **omliggende bewijs ontbrak**.

Les: een tool of een klik is niet genoeg — het gaat om de **bewijsketen eromheen**. Sterker bewijs = :

- **Identiteit:** akkoord alleen mogelijk achter een **persoonlijke login** (geen anonieme klik, geen gedeelde computer-sessie).

- **Tijd:** een **server-tijdstempel** (niet de klok van de browser — die is te vervalsen).
 - **Audit trail:** logboek van elke stap (getoond, gelezen, geklikt, bevestigd) met IP en tijdstip.
 - **Integriteit:** vastleggen wélke exacte versie is geaccordeerd, met een controlegetal (hash).
-

3. Jullie eigen idee beoordeeld (mail + reply + herinnering + bellen)

Het idee: na akkoord een bevestigingsmail met samenvatting → medewerker moet **replyen** (als tweestapsverificatie) → melding op kantoor → herinnering na 24 uur → bellen als derde stap.

Eerlijke beoordeling:

- **Bevestigingsmail: goed idee, houden.** Het is bekende best practice ("double opt-in"). Het levert **sterker bewijs** van instemming: het bewijst dat het mailadres bestaat, toegankelijk is, en dat iemand met toegang tot die mailbox actief bevestigde, met tijdstempel.
- **Reply als "2FA": nee, dat is géén echte tweede factor.** Replyen bewijst alleen mailbox-toegang — dezelfde zwakke factor als de klik zelf. Je verdubbelt dezelfde factor. Bovendien is e-mail-reply rommelig en manipuleerbaar (spoofing, doorstuurregels, een reply-lezer op kantoor is foutgevoelig).
- **Beter:** vervang "reply" door een **klik-link met een unieke code** in de mail (een zogenaamde magic link) **of een cijfercode (OTP)** die de medewerker intoetst. Het mooiste: koppel de bevestiging aan de **bestaande medewerker-login**. Dat is de sterkste identiteitsbinding.
- Kleine valkuil: sommige mailscanners openen links automatisch en "verbruiken" zo de code. Een in te typen cijfercode heeft dat probleem niet.
- **Herinnering na 24u + bellen: juridisch geen bewijs van akkoord, maar wél waardevol.** Geen reactie = geen akkoord (stilzwijgen telt niet). Maar deze stappen bewijzen dat de werkgever zich **aantoonbaar heeft ingespannen** om het akkoord te krijgen — belangrijk bij een arbeidsconflict of veiligheidsincident. **Leg die stappen dus óók vast** in dezelfde audit trail (wie, wanneer, uitkomst van het telefoontje).

4. Wat jullie al hebben (wie/wanneer/wat + SHA256) — dit is sterk

Het opslaan van **wie / wanneer / wat + een SHA256-controlegetal** is precies de goede aanpak.

- Een **SHA256-hash** is een uniek "vingerafdruk-getal" van het document. Verandert er later één komma, dan verandert het hele getal. Zo bewijs je dat het document **niet achteraf is gewijzigd**.
- **Beperking:** een hash alleen bewijst niet *wanneer* hij bestond, en niet dat jij hem niet later opnieuw hebt berekend. Maak hem daarom sterker:
- **Onafhankelijk tijdstempel (RFC 3161):** je stuurt alleen het controlegetal naar een onafhankelijke tijdstempel-dienst, die er een gecertificeerde datum bij zet en ondertekent. Dan is onweerlegbaar dat het getal vóór dat moment bestond — los van jouw eigen server. **Gratis dienst: FreeTSA.**
- **Ketening (hash chain):** elk nieuw akkoord-record neemt het controlegetal van het vorige mee. Dan kan niemand één oud record wijzigen zonder de hele keten te breken (het principe achter blockchain). Dit tilt jullie bewijs richting het niveau van een geavanceerde (AES) handtekening.

5. De drie opties

Optie A — Goedkoop: zelf inbouwen (SES+), aanbevolen voor de VCA-tool

Bouw het akkoord in de eigen web-app, met een stevige bewijsketen:

- Akkoord alleen achter de **persoonlijke login**.
- Vastleggen: user-ID, **server-tijdstempel**, exacte **documentversie + SHA256-hash**, IP + apparaat.
- **Bevestigingsmail** met samenvatting + **klik-link of cijfercode** (niet "reply").
- **Gratis RFC 3161-tijdstempel** (FreeTSA) op de hash + **ketening** van de records.
- **Onwijzigbare opslag** (append-only log) + herinnering-na-24u en telefoon-stap mee-loggen.

- **Kosten:** €0 aan licenties, alleen bouwtijd. (Tijdstempel gratis.)
- **Juridisch:** ruim voldoende voor interne HR/VGM/VCA-akkoorden.
- **Nadeel:** jullie onderhouden het zelf; bij betwisting moet jij het proces uitleggen (maar met bovenstaande is dat goed te doen).

Optie B — Midden: Nederlandse e-sign-tool (SES/AES)

Kant-en-klare tool die de handtekening + audit trail (evidence package) voor je regelt.

- **Voorbeelden (NL/EU):** ValidSign, Zynyo, Signhost/Entrust. Leveren SES én AES, met fraudebestendige audit trail en EU-opslag.
- **Prijsindicatie (geverifieerd waar publiek):** ValidSign gratis-plan (15 transacties), Pro **vanaf €27 per gebruiker/mnd**; Signhost/Entrust werkt met **credits** (prijs niet publiek); Scrive Essential **€21/mnd**, Business **€49/mnd**.
- **Wanneer:** als je geen zelfbouw wilt onderhouden, of AES wilt voor iets zwaardere stukken.

Optie C — Zwaar: gekwalificeerd (QES) via een erkende partij

De handtekening met identiteitscontrole (iDIN, itsme), **wettelijk gelijk aan een natte handtekening**; bij betwisting draait de bewijslast om.

- **Voorbeelden:** Scrive (is zelf gekwalificeerd), DocuSign QES-add-on (**+€10 per ontvanger**), Signhost met video-/eID-identificatie.
- **Wanneer:** alleen voor **hoog-risico documenten** — de arbeidsovereenkomst zelf, een vaststellingsovereenkomst. **Overkill** voor een toolbox-akkoord.

6. Concreet advies voor de VCA-tool

1. **Doe Optie A** voor alle interne akkoorden (reglement, veiligheid, PMO). Jullie hebben de kern (wie/wanneer/wat + SHA256) al — maak hem af met: login-koppeling, magic-link/OTP i.p.v. reply, gratis FreeTSA-tijdstempel, en ketening van records.
2. **Bewaar** de herinnering + het telefoon-moment in dezelfde audit trail — als bewijs van jullie inspanning.

3. Hou Optie B/C achter de hand voor échte contracten

(arbeids-/vaststellingsovereenkomst). Kies dan een NL-tool met AES, of QES bij grote gevolgen.

4. Laat het één keer door een arbeidsjurist bekijken voordat het live gaat — voor een waterdicht oordeel in de Nederlandse arbeidsrechtelijke context.

Bronnen (geverifieerd)

- Wettekst art. 3:15a BW (elektronische handtekening) — wetboekplus.nl / maxius.nl
- TRIP Advocaten — de 3 niveaus, bewijskracht en bewijslast: trip.nl/blogs/juridische-gevolgen-gebruik-elektronische-handtekening/
- De Clercq Advocaten — bewijslast per soort handtekening: declercq.com/kennisblog/2182-...
- VBV Advocaten — zaak Hof Arnhem-Leeuwarden 21-10-2025 (bewijs ontbrak): vbvadvocaten.nl/digitale-handtekening-onvoldoende-betrouwbaar/
- AWWN — bewijslast per niveau: awvn.nl/blog/elektronische-handtekening/
- EUR-Lex — Verordening 910/2014 (eIDAS): eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32014R0910
- DocuSign EU-prijzen + AES/QES-add-on: ecom.docusign.com/plans-and-pricing/esignature
- Scribe-prijzen + QES: scribe.com/pricing/esign-online
- ValidSign NL (SES/AES/QES, audit trail): validsign.eu/nl/
- Zynyo (niveaus + eID's): zynyo.com/identificatiemiddelen/
- FreeTSA — gratis RFC 3161-tijdstempel + commando's: freetlsa.org
- RFC 3161 uitleg: proofstamper.com/en/guide/rfc-3161-explained/
- Audit-trail-velden (checklist): useanvil.com/blog/engineering/e-signature-audit-trail-schema-events-json-checklist/
- Magic link vs OTP (valkuil mailscanners): scalekit.com/blog/otp-vs-magic-links-passwordless-authentication
- Double opt-in (AVG best practice): iubenda.com/en/blog/gdpr-double-opt-in-2/

Eerlijke kanttekeningen

- Er is **geen wet of rechtszaak die één vast niveau eist** voor VCA-toolbox of personeelsreglement. "SES volstaat" is een redenering op basis van de open norm (laag risico → licht niveau), geen expliciete regel.
- De **letterlijke tekst van art. 6:227a BW** (elektronische weg) en **eIDAS art. 25** is via meerdere bronnen bevestigd, maar niet woordelijk uit de primaire tekst overgenomen — check die nog even bij gebruik in een formeel/juridisch stuk.
- Voor een **waterdicht oordeel** in het Nederlandse arbeidsrecht is een jurist het beste ijkpunt; dit verslag is een goed onderbouwd advies, geen juridisch bindend advies.