



## Algemene voorwaarden met betrekking tot het KIND&GEZIN-certificaat voor de software leveranciers in de sector Kinderopvang

---

Het certificaat staat Het KIND&GEZIN-certificaat moet gezien worden als een digitaal identiteitsbewijs voor een natuurlijke persoon, rechtspersoon of feitelijke vereniging. Het KIND&GEZIN-certificaat moet behandeld worden met de nodige voorzorgen om misbruik van die identiteit te voorkomen.

Iedereen die een KIND&GEZIN-certificaat (hierna het certificaat genoemd) aanvraagt of gebruikt (hierna de aanvrager of de certificaathouder genoemd), zowel persoonlijk als in naam en voor rekening van een rechtspersoon of een feitelijke vereniging, is onderworpen aan de volgende voorwaarden:

De aanvrager van een certificaat heeft kennis van het gebruik van digitale certificaten en Public Key Infrastructure (PKI). Indien nodig laat de aanvrager zich hieromtrent informeren of bijstaan door deskundigen.

De aanvrager staat in voor de gegevens en sleutels die hij ter certificatie indient bij het KIND&GEZIN-platform en garandeert dat deze volledig en correct is.

Het is verboden het certificaat op enigerlei wijze te manipuleren.

De certificaathouder mag het certificaat uitsluitend gebruiken voor wettelijke en toegelaten doeleinden in overeenstemming met de geldende overeenkomsten tussen Kind&Gezin en de organisatoren Kinderopvang..

De certificaathouder moet het KIND&GEZIN-platform onmiddellijk informeren over iedere wijziging in de informatie die eerder werd doorgestuurd. De certificaathouder dient hiervoor contact op te nemen met de veiligheidsconsulent (per e-mail naar [ICT.Ontwikkeling.Software.box@kindengezin.be](mailto:ICT.Ontwikkeling.Software.box@kindengezin.be)).

De certificaathouder moet het gebruik van het certificaat onmiddellijk beëindigen als

- enige informatie in het certificaat niet meer valide is of
- wanneer het certificaat om welke reden dan ook ongeldig is.

Wanneer het het certificaat niet langer geldig is, verwijdert de certificaathouder het certificaat en het bijhorende sleutelpaar uit de verschillende toepassingen en apparaten waar het werd geïnstalleerd.

De certificaathouder vraagt minstens 10 werkdagen voor het verlopen van het certificaat een nieuw certificaat volgens de geldende procedure aan te vragen. De geldigheidsduur (38 maanden) van een certificaat kan niet verlengd worden.

De certificaathouder voorkomt dat de private sleutel behorende bij het certificaat of het certificaat zelf wordt gecompromitteerd, verloren, bekend gemaakt, gewijzigd of op enig andere manier wordt misbruikt.

Als het certificaat of de bijbehorende private sleutel gecompromitteerd is, beëindigt de certificaathouder ogenblikkelijk en definitief het gebruik ervan.

De certificaathouder is aansprakelijk voor alle (rechtstreekse of onrechtstreekse) schade door elk al dan niet geoorloofd gebruik ervan, met inbegrip van elk gebruik door derden tot op het tijdstip waarop het certificaat geïnactiveerd werd.

Bronverwijzingen:

<http://repository.pki.belgium.be/>

[http://nl.wikipedia.org/wiki/Digitaal\\_certificaat](http://nl.wikipedia.org/wiki/Digitaal_certificaat)

[http://nl.wikipedia.org/wiki/Public\\_Key\\_Infrastructure](http://nl.wikipedia.org/wiki/Public_Key_Infrastructure)