

Algemene Voorwaarden voor het gebruik van Certificaten bij ZetesConfidens vertrouwensdiensten

1. Deze Algemene Voorwaarden zijn van toepassing op het gebruik van certificaten (hierna aangeduid als de "Certificaten") voor vertrouwensdiensten die worden verleend door ZetesConfidens (onderdeel van Zetes nv, Straatsburgstraat 3, 1130 Brussel, KBO 0408.425.626).
2. Het Certificaat staat op naam van de houder (hierna de "Gebruiker") en wordt verstrekt aan natuurlijke personen op vraag van een Inschrijver op de vertrouwensdienst. De Inschrijver is de partij door wiens bemiddeling de Gebruiker zijn Certificaat bekam. Indien de Gebruiker zich rechtstreeks tot de vertrouwensdienstenverlener wendde, is hij tevens de Inschrijver.
3. De Certificaten zijn onderdeel van een Publieke Sleutel Infrastructuur (PKI) opgezet door de vertrouwensdienstenverlener. Alle relevante documenten om de werking van een Certificaat in de PKI te duiden (waaronder de Certification Practice Statement CPS en de Certificate Policy CP) zijn publiek beschikbaar op <https://repository.confidens.zetes.com/>. De Gebruiker aanvaardt dat instructies vervat in deze CPS en CP deel uitmaken van de Algemene Voorwaarden.
4. De Gebruiker dient deze Algemene Voorwaarden te aanvaarden vooraleer hij zijn Certificaten ontvangt of in gebruik neemt. De Gebruiker kijkt na of de informatie over de Certificaten vermeld op de ontvangstmelding overeenstemt met zijn aanvraag. Door de ontvangstmelding te tekenen of te bevestigen met een code sluit hij een Gebruikersovereenkomst af en bevestigt de Gebruiker dat hij deze Algemene Voorwaarden, het Privacybeleid en de informatie over de Certificaten gelezen heeft, en gaat hij ermee akkoord dat deze Algemene Voorwaarden op hem van toepassing zijn.
5. De prijs voor het bekomen van een Certificaat wordt vastgelegd met de Inschrijver en indien doorgerekend voorafgaand aan de aanvraag meegedeeld aan de Gebruiker. Bij vervanging van Certificaten kunnen kosten in rekening worden gebracht. In voorkomend geval zullen deze toepasselijke kosten steeds vooraf aan de Gebruiker worden getoond.
6. Certificaten hebben een welbepaald gebruik dat vaak door hun benaming kenbaar wordt gemaakt. De gebruiksdoeleinden zijn steeds aangegeven in het Certificaat.
7. Een Certificaat en de bijhorende private sleutel is strikt persoonlijk. Het gebruik kan door de Gebruiker niet gedelegeerd

worden aan een derde. De Gebruiker mag zijn Certificaten alleen zelf aanwenden door middel van sterke authenticatie (2FA). De Gebruiker moet zijn private sleutels afschermen, en zal verantwoordelijk zijn voor elk gebruik. Indien de Gebruiker weet heeft of gegronde reden heeft om te vermoeden dat zijn private sleutel(s) of PIN-code(s) bekend zou(den) kunnen zijn bij derden of de geldigheid van zijn Certificaten op andere wijze aangetast zouden zijn, moet hij de Inschrijver hiervan verwittigen en de revocatie van de Certificaten aanvragen.

8. De private sleutels dienen beveiligd te worden conform de vereisten voor het beoogde gebruik, zoals bepaald in de respectievelijke specifieke gebruiksvoorwaarden en de CP en CPS. Naargelang het vereiste veiligheidsniveau en functionele vereisten wordt de sleutel opgeslagen in een beveiligd sleutelbestand of in speciale beveiligde hardware zoals een smartcard of equivalent of een HSM. Naargelang het vereiste veiligheidsniveau en functionele vereisten wordt de sleutel gegenereerd in software of in beveiligde cryptografische hardware. Naargelang het vereiste veiligheidsniveau en functionele vereisten zijn de methodes voor de creatie en opslag van de sleutel onder controle van de Gebruiker, van de Inschrijver of van de Vertrouwensdienstenverlener. In alle gevallen zal de Vertrouwensdienstenverlener geen Certificaat uitreiken indien de gebruikte middelen en methodes niet voldoen aan het vereiste veiligheidsniveau voor het betreffende Certificaat en de gebruiksdoeleinden van het Certificaat.
9. Certificaten die door de vertrouwensdienstenverlener zelf worden opgeslagen in een beveiligde omgeving kunnen door de Gebruiker op afstand worden gebruikt. Het gebruik op afstand van Certificaten wordt steeds beschreven in een apart document (zoals een Server Signing Practice Statement) dat ook beschikbaar wordt gesteld aan de Gebruiker.
10. Het opzetten van de vertrouwensdienst vereist de verwerking van bepaalde persoonsgegevens. Dat gebeurt in overeenstemming met de bepalingen van het Privacybeleid ter beschikking gesteld bij de aanvraag. De Gebruikers bevestigen bijgevolg dat zij het Privacybeleid gelezen en begrepen hebben en gaan akkoord dat het Privacybeleid op hen van toepassing is.
11. Geen enkel ander gebruik van de Certificaten dan beschreven in paragrafen 7 en 8 is toegelaten. Elk gedrag dat strijdig is met deze Algemene Voorwaarden of de toepasselijke wetgeving is verboden. Elk gebruik van een Certificaat in strijd met deze Algemene Voorwaarden gebeurt dan ook volledig op eigen risico en zonder enige garantie. De vertrouwensdienstenverlener behoudt zich het recht voor op vraag van de Inschrijver of de Gebruiker zelf of op eigen initiatief een certificaat te herroepen

overeenkomstig de documenten in paragraaf 3. Een herroepen Certificaat laat geen geldig gebruik meer toe.

12. De Gebruikers van de Certificaten bevestigen en waarborgen dat de informatie die zij bij de aanvraag verstrekt hebben en zoals deels op de Gebruikersovereenkomst weergegeven correct was en dat zij gerechtigd zijn om de Certificaten te gebruiken.
13. De Gebruikers brengen de Inschrijver of de vertrouwensdienstenverlener onverwijld op de hoogte via de kanalen die daarvoor zijn aangeduid bij verlies of diefstal van sleutels of Certificaten, of bij wijziging van enige informatie op de Certificaten zoals hierboven aangegeven. De Gebruikers zijn verantwoordelijk voor enig onrechtmatig gebruik van de kaart door derden indien zij talmen bij het voldoen aan deze meldingsplicht.
14. De vertrouwensdienstenverlener en de Inschrijver bieden geen enkele waarborg bij schending van de Algemene Voorwaarden en aanvaarden geen enkele aansprakelijkheid indien de Gebruiker daaraan niet voldoet.
15. In geen enkel geval, behalve indien wettelijk verplicht onder de toepasselijke wetgeving of indien schriftelijk overeengekomen, kan de vertrouwensdienstenverlener op enige wijze aansprakelijk worden gehouden voor de vergoeding van enige schade, inclusief voor algemene schade, speciale of gevolgschade, als gevolg van het gebruik of de onmogelijkheid van het gebruik van de Certificaten (met inbegrip van maar niet beperkt tot het verlies of de beschadiging van data toebehorend aan de Gebruikers of aan derden).
16. Indien die uitsluiting en beperking van aansprakelijkheid geen of geen volledige uitwerking kan krijgen onder het toepasselijke recht, zullen uitspraakdoende rechtbanken het toepasselijke recht gebruiken op een wijze die het nauwst aansluit bij een volledige uitsluiting van burgerlijke aansprakelijkheid in verband met het gebruik van de Certificaten.
17. Deze Algemene Voorwaarden zijn onderworpen aan het Belgische recht. Geschillen over de Algemene Voorwaarden zijn onderworpen aan de uitsluitende bevoegdheid van de rechtbanken van Brussel, België.
18. Deze Algemene Voorwaarden (inclusief de documenten in paragraaf 3 en het Privacybeleid) kunnen worden aangevuld, herzien of bijgewerkt. De Gebruikers aanvaarden dat het gebruik van de Certificaten steeds onderworpen is aan de versie van de Algemene Voorwaarden die bekendgemaakt en van toepassing is op het moment van het gebruik.

Conditions générales pour l'utilisation des Certificats pour les services de confiance de ZetesConfidens

1. Les présentes Conditions générales s'appliquent à l'utilisation des certificats (ci-après les « Certificats ») fournis par le prestataire de services de confiance ZetesConfidens (division de Zetes sa, 3 rue de Strasbourg à 1130 Bruxelles, BCE 0408.425.626).
2. Le Certificat est libellé au nom du porteur (ci-après le « Porteur ») et est remis à une personne physique à la demande du Demandeur du service.
3. Les Certificats font partie d'une Infrastructure à Clés Publiques (ICP) organisée par le prestataire de services de confiance. Tous les documents pertinents pour décrire le fonctionnement d'un Certificat dans l'ICP (y compris le Certification Practice Statement CPS et le Certificate Policy CP) sont publiquement accessibles sur <https://repository.confidens.zetes.com/>. Le Porteur accepte que les instructions incluses dans ces CPS et CP fassent partie des Conditions générales.
4. Le Porteur doit accepter ces Conditions générales avant de recevoir ses Certificats. Le Porteur s'assure que les informations relatives aux Certificats figurant sur le formulaire de réception correspondent à sa demande. En signant pour réception ou en confirmant avec un code le Porteur ratifie une Convention utilisateur et il confirme qu'il a lu les Conditions générales, la Politique de confidentialité et les informations relatives aux Certificats, et qu'il accepte que ces Conditions générales s'appliquent à lui.
5. Le prix pour l'obtention d'un Certificat est fixé en accord avec le Demandeur et au cas où le prix est à charge du Porteur il est communiqué à celui-ci avant la demande. Des frais pourront être portés en compte en cas de remplacement de Certificats. Le cas échéant, ces frais seront toujours présentés préalablement au Porteur.
6. Les Certificats ont une utilisation spécifique, souvent reconnaissable à leur dénomination. Leurs finalités d'usage est décrit dans le Certificat.
7. Le Certificat et sa clé secrète liée sont strictement personnels. Le Porteur ne peut en déléguer l'utilisation à un tiers. Le Porteur est seul autorisé à utiliser ses Certificats par voie d'authentification forte (2FA). Le Porteur doit garder ses clés privées secrètes; à défaut, il sera responsable de toute éventuelle utilisation. Si le Porteur a connaissance, ou s'il a des

motifs fondés de supposer que sa ou ses clés privées ou codes PIN sont ou seraient connus par des tiers, ou que la validité de ses Certificats serait compromise d'une manière ou d'une autre, il est tenu d'en avertir le Demandeur et de demander la révocation des Certificats.

8. Les clés privées doivent être sécurisées conformément aux exigences relatives à l'utilisation envisagée, telles que définies dans les conditions d'utilisation spécifiques respectives, ainsi que dans le CP et le CPS. En fonction du niveau de sécurité requis et des exigences fonctionnelles, la clé est stockée dans un fichier de clé sécurisé ou dans un dispositif hautement sécurisé, tel qu'une carte à puce ou un équivalent, ou un HSM. En fonction du niveau de sécurité requis et des exigences fonctionnelles, la clé est générée dans un logiciel ou dans un dispositif cryptographique sécurisé. En fonction du niveau de sécurité requis et des exigences fonctionnelles, les méthodes de création et de stockage de la clé sont sous le contrôle du Porteur, du Demandeur ou du Prestataire de services de confiance. Dans tous les cas, le Prestataire de services de confiance n'émettra pas de Certificat si les moyens et les méthodes utilisés ne répondent pas au niveau de sécurité requis pour le Certificat concerné et aux fins de l'utilisation de celui-ci.
9. Les Certificats sauvegardés auprès du prestataire de service sont mis à disposition du Porteur sous son contrôle à distance. L'utilisation à distance des Certificats est décrite dans un document séparé (comme un Server Signing Practice Statement) disponible pour le Porteur.
10. L'organisation du service de confiance requiert le traitement de certaines données à caractère personnel. Ce traitement s'effectue dans le respect des dispositions de la Politique de confidentialité mise à disposition lors de la procédure d'inscription. Le Porteur confirme par conséquent qu'il a lu et compris la Politique de confidentialité, et accepte qu'elle s'applique à lui.
11. Aucune utilisation des Certificats autre que celle décrite aux paragraphes 7 et 8 n'est autorisée. Tout comportement en violation des présentes Conditions générales et/ou de la loi applicable est proscrit. Toute utilisation d'un Certificat en violation des présentes Conditions générales s'effectue par conséquent aux risques du Porteur et sans la moindre garantie. Le prestataire de services de confiance se réserve le droit de révoquer un Certificat, à la demande du Demandeur, du Porteur lui-même, ou à sa propre initiative, conformément aux

documents mentionnés au paragraphe 3. Un Certificat révoqué ne peut plus être utilisé valablement.

12. Les Utilisateurs des Certificats confirment et garantissent que les informations qu'ils ont fournies lors de la demande et qui sont déjà partiellement reprises dans la Convention utilisateur sont exactes et qu'ils sont habilités à utiliser les Certificats.
13. Les Utilisateurs informeront sans délai le Demandeur ou le prestataire de service de confiance, via les canaux indiqués, de la perte ou du vol de leur Certificat ou des clés privées, ou en cas de modification de toute information sur les Certificats comme indiqué ci-dessus. Les Porteurs sont responsables de toute utilisation illégitime par des tiers s'ils manquent à leur obligation de notification décrite ci-avant.
14. Ni le Prestataire de services de confiance ni le Demandeur fournissent de garantie en cas de violation des Conditions générales et déclinent toute responsabilité si le Porteur ne s'y conforme pas.
15. En aucun cas, sans préjudice d'une obligation légale en vertu de la législation en vigueur ou d'un accord écrit, le prestataire de services de confiance ne peut, de quelque manière que ce soit, être tenu pour responsable pour l'indemnisation de quelque dommage que ce soit, y compris pour des dommages généraux, spéciaux ou consécutifs résultant de l'utilisation ou de l'impossibilité d'utiliser les Certificats (y compris, mais sans s'y limiter, la perte ou la détérioration de données appartenant aux Porteurs ou à des tiers).
16. Si l'exclusion et la limitation de responsabilité ne peuvent produire d'effet, ou uniquement un effet partiel, en vertu du droit applicable, les tribunaux compétents feront appel au droit applicable de la manière correspondant le plus étroitement à une exclusion de responsabilité civile à l'égard de l'utilisation des Certificats.
17. Les présentes Conditions générales sont soumises au droit belge. Tout litige relatif aux Conditions générales relève de la compétence exclusive des tribunaux de Bruxelles, Belgique.
18. Les présentes Conditions générales (y compris les documents mentionnés au paragraphe 3 et la Politique de confidentialité) peuvent être complétées, remaniées ou mises à jour. Les Porteurs acceptent que l'utilisation des Certificats soit toujours soumise à la version des Conditions générales publiées et d'application au moment de l'utilisation.