Business Dashboard Overeenkomst
Voorwaarden Beveiliging

Geregistreerd te Leuven op 22 februari 2018 en van kracht met ingang van 26 februari 2018.

Deze uitgave telt 7 bladzijden.

1 Definities

De definities uit de Business Dashboard Overeenkomst – Algemene bepalingen zijn ook van toepassing op deze Business Dashboard Overeenkomst – Voorwaarden Beveiliging tenzij er uitdrukkelijk van wordt afgeweken. De definities kunnen zonder onderscheid in het meervoud en het enkelvoud gebruikt worden.

Aanvraagformulier

Het deel van de Business Dashboard Overeenkomst dat door de Klant(en) wordt ondertekend,waarin de Klant(en) worden geïdentificeerd, de afgenomen Diensten en de toepasselijke contractvoorwaarden worden aangeduid.

Authenticatie

Het proces waarbij een identiteit wordt vastgesteld, op basis van het bezit van een betrouwbaar bewijsstuk.

Bijlagen

Documenten die de Partijen in wederzijdse overeenstemming aan deze Business Dashboard Overeenkomst –Voorwaarden Beveiliging aanhechten. Alle Bijlagen zijn onderworpen aan deze Business Dashboard Overeenkomst – Voorwaarden Beveiliging.

Certificatie-autoriteit of CA

De autoriteit die belast is met certificatie. Op het moment van ondertekening van deze Overeenkomst is Isabel NV, gevestigd te 1000 Brussel, Keizerinlaan 13-15, verantwoordelijk voor het uitgeven en het beheer van de Certificaten. De certificatiediensten worden verleend conform deze Overeenkomst en de voorwaarden van de toepasselijke Certificate Policy, zoals hieronder omschreven.

Certificate Policy of CP

De PKI@CBC Certificate Policy, waarin de regels vervat zijn voor de toepasselijkheid van een certificaat op een bepaalde gemeenschap en/of categorie toepassingen met gemeenschappelijke beveiligingsvereisten. De volledige tekst van de CP is beschikbaar op de website: www.kbc.com/certificate-policy.

De Certificate Policy bepaalt voornamelijk welke de basisverplichtingen zijn van de CA en de andere partijen die betrokken zijn bij de CBC public key infrastructure (PKI). De PKI is een systeem waarmee de uitgifte en het beheer van Digitale Certificaten kan worden gerealiseerd.

Certificaat

Een Digitaal Certificaat dat is uitgegeven door de CA.

Certificate Revocation List

Een lijst van herroepen Certificaten digitaal ondertekend door de uitgevende CA.

Connected Card Reader of CCR

De kaartlezer die verbonden is met de computer van de Gebruiker en gebruikt wordt voor het lezen van een smartcard, zoals de CBC-eBusinesskaart of de CBC eBusiness Portal Kaart.

Digitaal certificaat

Een computerbestand dat de publieke sleutel van de Gebruiker-certificaathouder bevat, zijn identiteit en andere informatie (zoals de geldigheidsduur van het certificaat, de identiteit van de uitgever, de locatie van de CertificateRevocationList), en een samenvatting van bovenstaande gegevens gereduceerd tot een unieke code en versleuteld met de private sleutel van de Certificatieautoriteit (CA).

Het Digitaal certificaat wordt uitgegeven en beheerd door de CA. De CA waarborgt de integriteit en authenticiteit van het Digitaal Certificaat.

Digitale toepassing(en)

De Diensten en Dashboard functionaliteiten die achter het Dashboard zitten en die deel uitmaken van de Business Dashboard Overeenkomst, en waarvoor de Klant(en) en/of de Gebruiker gebruik maak(t)(en) van de Business Dashboard Security.

Documentatie

De documentatie toegevoegd aan of waarnaar in de Business Dashboard Overeenkomst – Voorwaarden Beveiliging verwezen wordt, zoals de CP.

eBusiness Portal Kaart

Een chipkaart waarop de Private Sleutel van de gecertificeerde Gebruiker is opgeslagen en waarmee de gecertificeerde Gebruiker een elektronische handtekening aanmaakt.

Business Dashboard Security

De Toegangs- en ondertekeningsmiddelen waarmee de Gebruiker zich kan authenticeren en een elektronische handtekening kan plaatsen. Deze elektronische handtekening mag uitsluitend worden gebruikt in het kader van de Digitale toepassingen en onder bepaalde voorwaarden voor e-Government-toepassingen in België.

De Business Dashboard Security stelt de Gebruiker in staat om:

i. Toegang te hebben tot de Digitale toepassingen die vermeld zijn in het Aanvraagformulier;

ii. Opdrachten te initiëren en te bevestigen, en onder bepaalde voorwaarden gebruik te maken van e-Government-toepassingen.

Geheime code

De persoonlijke en vertrouwelijke identificatiecode die de Gebruiker moet invoeren in CBC Sign om de Gebruiker te identificeren of Opdrachten te tekenen.

Business Dashboard Overeenkomst
Voorwaarden Beveiliging

Gebruiker

Een natuurlijke persoon of een afdeling van de Klant, naar behoren geïdentificeerd en gemachtigd om binnen het toepassingsgebied van deze Overeenkomst in naam en voor rekening van de Klant gebruik te maken van de door de Klant aangeduide Diensten en Dashboard functionaliteiten binnen de Overeenkomst. Een Gebruiker die op afstand werd geïdentificeerd door de Klant, en geen volledig geïdentificeerde CBC-klant is, wordt voor het gebruik van CBC Sign aangeduid als een CBC Sign Light Gebruiker.

Jailbreak / rooting

Een handeling die het mogelijk maakt om de beveiliging van een Toestel (waarbij we spreken van een jailbreak bij een iPhone en rooting bij een Android- of andere smartphone) te omzeilen en hierop softwaretoepassingen te laden die door de officiële distributeur van het Toestel niet erkend/goedgekeurd zijn. Het Toestel wordt hierdoor meer vatbaar voor virussen en malware (zijnde software die is bedoeld om computers en computersystemen te beschadigen of uit te schakelen).

Kaart

De CBC-Bankkaart waarvan de Gebruiker houder is en die hij samen met de bijhorende pincode en de Kaartlezer gebruikt om zich aan te melden in bepaalde Digitale toepassingen. Het gebruik van de Kaart wordt beheerst door het Reglement CBC-Bankkaart.

Kaartlezer

Een toestelletje dat in combinatie met de Kaart en de bij de Kaart horende pincode een nieuwe code genereert waarmee de Gebruiker zich kan aanmelden en Opdrachten kan ondertekenen in bepaalde Digitale toepassingen.

CBC-e-Businesskaart

Een smartcard met een private sleutel die een digitale handtekening genereert en waarmee de Gebruiker (i) zich aanmeldt in het Dashboard en de Digitale toepassing(en) en (ii) Opdrachten kan ondertekenen. Een bijgeleverd certificaat bevestigt dat de Gebruiker-ondertekenaar houder is van een private en publieke sleutel.

Elk te ondertekenen bericht of opdracht wordt gereduceerd tot een unieke code die wordt versleuteld met de private sleutel van de Gebruiker, en kan enkel worden geverifieerd met de publieke sleutel van de Gebruiker. De publieke sleutel kan door iedereen worden opgevraagd.

CBC-Mobile app

Het geheel van procedures, overeengekomen tussen de Gebruiker en de Bank, die toegang bieden tot de diensten van CBC Mobile via een eigen Toestel en die het de Gebruiker mogelijk maken om mobiel te bankieren.

CBC Sign

Het Toegangs- en ondertekeningsmiddel waarbij de Gebruiker via de app CBC Sign geïnstalleerd op een mobiel Toestel (smartphone), en gescheiden van de Digitale toepassing,

- geauthenticeerd wordt (nagaan of de Gebruiker daadwerkelijk is wie hij beweert te zijn);
- opdrachten in de Digitale toepassing kan ondertekenen.

CBC

De Bank, de Verzekeraar of de entiteit die onderdeel is van de CBC -groep en die optreedt als de distributeur van de Digitale toepassing en de Business Dashboard Security.

Opdracht

Een door de Gebruiker geïnitieerde opdracht, met inbegrip van maar niet beperkt tot betalings- of beleggingstransacties, en elke instructie tot aanvaarding van een nieuw of gewijzigd contract met CBC.

Overeenkomst

De Overeenkomst die bestaat uit:

- het Aanvraagformulier;
- de Business Dashboard Overeenkomst – Algemene Bepalingen;
- de Applicatiecontracten;
- de Business Dashboard Overeenkomst – Bijzondere Bepalingen;
- de Business Dashboard Overeenkomst – Voorwaarden Beveiliging;
- de Documentatie en de Bijlagen;

en alle wijzigingen en aanvullingen die hieraan op een later tijdstip schriftelijk kunnen worden overeengekomen tussen de Partijen.

Partij en Partijen

De Klant of CBC afzonderlijk aangeduid als Partij en gezamenlijk als Partijen.

Private sleutel

De sleutel die alleen door de Gebruiker gekend is en wordt gebruikt om de informatie te coderen (vercijferen) of te ondertekenen.

Publieke sleutel

De sleutel die openbaar is en die gebruikt wordt om de informatie weer te decoderen (ontcijferen) of de identiteit van de Gebruiker te verifiëren.

QR-code

Een tweedimensionale streepjescode die toelaat om gebruiksvriendelijk en snel (digitale) informatie over te dragen/in te lezen.

Registratie-autoriteit (RA)

De Bank en/of de Verzekeraar, of enig andere entiteit van de KBC-groep die vaststelt aan welke Gebruiker een Digitaal Certificaat kan worden verstrekt en instaat voor de identificatie en registratie van de Gebruiker. De RA ondertekent geen certificaten en geeft deze niet uit. De RA kan assisteren bij het aanvraag-en/of herroepingsproces van certificaten, conform de bepalingen van de toepasselijke CP.

Toegangs- en ondertekeningsmiddelen

De vereiste middelen, waarmee (i) de Gebruiker geauthenticeerd wordt en toegang verkrijgt tot de Digitale toepassing, en (ii) Opdrachten in de Digitale toepassing kan ondertekenen, en waarvoor de Gebruiker ofwel zelf een contract heeft gesloten met CBC, ofwel werd aangeduid als gemachtigd Gebruiker door de Klant. Een overzicht van deze Digitale toepassingen is te vinden op www.cbc.be/sign in het Aanvraagformulier.

Toestel

De smartphone waarop u de CBC Sign app kunt downloaden. De vereisten waaraan dat Toestel moet voldoen, staan op www.cbc.be/sign en op https://entreprendre.cbc.be/exigencestechniques.

2 Algemene bepalingen

2.1 Algemeen

De onderhavige Business Dashboard Overeenkomst – Voorwaarden Beveiliging maken deel uit van de Voorwaarden beveiliging in de Algemene Bepalingen van de Overeenkomst en bepalen de rechten en plichten van respectievelijk CBC, de Klant en de Gebruiker met betrekking tot het gebruik van de Business Dashboard Security.

2.2 Aansprakelijkheid van Partijen

Partijen erkennen dat de aansprakelijkheidsclausules, in het bijzonder de aansprakelijkheidsbeperkingen die zijn opgenomen in de Overeenkomst van toepassing zijn op de Business Dashboard Security.

2.3 Intellectuele Eigendomsrechten

CBC of haar derde licentiegever is en blijft eigenaar van de Intellectuele Eigendomsrechten en knowhow die verbonden zijn aan de Business Dashboard Security. Aan de Klant en/of de Gebruikers worden geen andere rechten toegekend dan de rechten die uitdrukkelijk in de Overeenkomst zijn vermeld.

Voor zover CBC software of Documentatie beschikbaar stelt in het kader van de levering van Business Dashboard Security, verleent CBC aan de Klant voor iedere Gebruiker een niet-overdraagbare, beperkte en niet-exclusieve licentie voor het gebruik van de Business Dashboard Security. Dit gebruik is beperkt tot de eigen bedrijfsdoeleinden van de Klant. De Klant dient alle nodige maatregelen te treffen om de Intellectuele Eigendomsrechten van CBC met betrekking tot de Business Dashboard Security te beschermen.

Ingeval van een klacht van een derde in verband met een inbreuk door CBC op de Intellectuele Eigendomsrechten van derden, verbindt de Klant zich ertoe om CBC onmiddellijk op de hoogte te stellen van een dergelijke klacht, om alle informatie en ondersteuning te verschaffen en om CBC het recht te verlenen om gerechtelijke procedures en onderhandelingen te voeren. Indien naar het oordeel van CBC een programma inbreuk gemaakt kan hebben op de Intellectuele Eigendomsrechten van een derde, dan zal CBC, uitsluitend ter harer beoordeling, de keuze maken om hetzij het inbreuk-makende programma zodanig aan te passen dat er geen sprake meer is van een inbreuk, hetzij het recht voor de Klant te verkrijgen om het gebruik van het programma voort te zetten, hetzij, indien naar het oordeel van CBC geen van deze alternatieven haalbaar is, om het gebruiksrecht voor het desbetreffende programma te beëindigen en eventuele vergoedingen die door de Klant voor dat programma betaald zijn terug te betalen.

2.4 Elektronische handtekening, bewijsvoering en kennisgeving

De Partijen komen overeen dat de elektronische handtekening die aangemaakt is door een Gebruiker volgens de geëigende procedures, gelijkgesteld wordt met een handgeschreven handtekening en aan de vereisten voldoet van artikel 1322, lid 2, van het Belgische Burgerlijk Wetboek. Dit geldt voor de relatie tussen CBC en de Klant.

De Partijen aanvaarden tevens dat aan de elektronische handtekening in alle gevallen alle rechtsgevolgen zijn verbonden die daaraan door de wet worden toegekend ten opzichte van CBC, haar Klanten en derden.

Als bewijs van elektronische berichten, verbindingen, transacties tussen de Klant en CBC zullen gelden de logs en transactiebestanden die elektronisch bewaard worden door CBC. De Klant aanvaardt de bewijskracht van deze gegevens. Deze manier van bewijslevering verhindert partijen niet om ieder hun eigen bewijs te leveren met gebruikmaking van de toegestane wettelijke middelen.

CBC registreert toegang tot de Digitale toepassingen door middel van de Business Dashboard Security. CBC houdt een logboek bij waarin alleen de gegevens worden opgeslagen die verband houden met het gebruik van de Business Dashboard Security. Dit logboek kan op papier of op ieder ander type gegevensdrager gereproduceerd worden. Het logboek levert het bewijs dat toegang is verkregen tot de Digitale toepassingen, tenzij de Klant het tegendeel kan bewijzen.

2.5 Verplichtingen van de Klant

2.5.1. Algemeen

De Klant ziet erop toe dat de Business Dashboard Security gebruikt wordt in overeenstemming met deze Algemene Voorwaarden, de Technische Vereisten, de nationale en internationale wetgeving en, in het algemeen, op een verantwoorde manier, uitsluitend voor geoorloofde doeleinden en zonder inbreuk te plegen op de rechten van derden.

CBC informeert de Klant en de Gebruikers over de veiligheidsvoorschriften en de te nemen maatregelen bij het gebruik van het Dashboard en de achterliggende Digitale Toepassingen via de Business Dashboard Overeenkomst – Voorwaarden Beveiliging, de Bijzondere Bepalingen van toepassing op de Digitale toepassingen en de webpagina's vermeld in artikel 2.6. De Klant en de Gebruikers worden geacht deze webpagina's regelmatig, en minstens één maal per maand, te raadplegen.

Het is de Klant en de Gebruikers niet toegestaan om wijzigingen aan te brengen aan de Business Dashboard Security. De Klant is aansprakelijk voor alle eventuele schade die kan voortvloeien uit aangebrachte wijzigingen, of uit het onrechtmatig of onjuist gebruik ervan door de Klant of zijn Gebruikers. De Business Dashboard Security wordt door de Klant geïnstalleerd. Onder geen enkele omstandigheid zal CBC aansprakelijk gehouden worden voor de gevolgen van fouten of nalatigheden die tijdens deze installatie begaan kunnen worden door de Klant of een derde.

2.5.2. Uitrusting van de Klant

De Klant verbindt zich ertoe enkel hard- en software te gebruiken die voldoet aan de hem door CBC kenbaar gemaakte Technische Vereisten noodzakelijk voor het gebruik van de Business Dashboard Security. CBC behoudt zich het recht voor deze Technische Vereisten van tijd tot tijd te wijzigingen.

De kosten van aankoop, installatie en werking van de Business Dashboard Security zijn volledig voor rekening van de Klant.

2.5.3. Beveiliging en beheer van de Toegangs-en ondertekeningsmiddelen

Tenzij uitdrukkelijk anders bepaald in de Bijzondere Bepalingen, zijn de Toegangs- en ondertekeningsmiddelen strikt persoonlijk. De Klant is verantwoordelijk voor de bewaring, vertrouwelijkheid, veiligheid en passend gebruik van de Toegangs- en ondertekeningsmiddelen door de Klant zelf en zijn Gebruikers en verbindt zich ertoe om alle nodige stappen te ondernemen om te voorkomen dat niet-bevoegde derden er kennis van kunnen nemen of gebruik van kunnen maken.

Ingeval van verlies, diefstal, inbreuk op de vertrouwelijkheid of elk risico van misbruik van de Toegangsmiddelen- en ondertekeningsmiddelen, of ingeval van verlies of diefstal van zijn Toestel dienen respectievelijk de Klant en de Gebruiker de volgende instanties daarvan onmiddellijk in kennis te stellen:

- CBC op het nummer 0800 65 650;
- de RA in geval van gebruik van de CBC-eBusinesskaart of de CBC eBusiness Portal Kaart zoals bepaald in de respectievelijke CPs.

De Klant en/of de Gebruiker leggen best ook een klacht neer bij de politie.

De Klant is tot aan het moment van kennisgeving volledig en onvoorwaardelijk aansprakelijk voor elk gebruik van de Digitale toepassingen, evenals voor schadelijke gevolgen die daar direct of indirect uit kunnen voortvloeien.

Na de kennisgeving draagt de Klant geen risico meer voor eventuele schade, behalve in geval van fraude, opzet of grove fout of poging daartoe.

Indien CBC enige reden heeft om te vermoeden dat er inbreuk is gemaakt op de vertrouwelijkheid en/of beveiliging van de Toegangsmiddelen- en ondertekeningsmiddelen of dat er misbruik wordt gemaakt van de Digitale toepassingen kan CBC de toegang tot de Digitale toepassingen opschorten.

Indien de Klant gebruik maakt van Toegangs- en ondertekeningsmiddelen gebruik makend van een Certificaat, moet de Klant ingeval van diefstal, verlies of enig ander vastgesteld misbruik of enige twijfel hieromtrent, of wanneer de gegevens op het Certificaat niet meer actueel zijn, het Certificaat herroepen overeenkomstig de procedure opgenomen in de CP. De Klant is verantwoordelijk voor alle schade die hijzelf, CBC of derden als gevolg van een niet- of laattijdige herroeping zouden lijden.

2.6 Verplichtingen van CBC

CBC verbindt zich ertoe om deze Overeenkomst als een goede huisvader uit te voeren. CBC zal de nodige maatregelen nemen om de continuïteit van de Business Dashboard Security te garanderen. CBC kan niet garanderen dat de Business Dashboard Security voldoet aan de specifieke verwachtingen, doelstellingen of vereisten van de Klant of diens Gebruikers.

CBC informeert de Klant en de Gebruikers over de veiligheidsvoorschriften en de te nemen maatregelen bij het gebruik van het Dashboard en de achterliggende Digitale Toepassingen via de Business Dashboard Overeenkomst – Voorwaarden Beveiliging, de Bijzondere Bepalingen van toepassing op de Digitale toepassingen en volgende webpagina's:

- dringende veiligheidsberichten op de aanmeldpagina's van het Dashboard: https://entreprendre.cbc.be en www.cbccorporate.be
- algemene veiligheidsbewustzijn en concrete veiligheidstips: https://secure4u.cbc.be
- specifieke veiligheidsvereisten met betrekking tot de infrastructuur van de gebruiker (als onderdeel van de systeemvereisten): https://entreprendre.cbc.be/exigencestechniques.

Alleen de Klant, en geenszins CBC, dient na te gaan dat het gebruik van Business Dashboard Security door de Klant voldoet aan alle wet- en regelgeving, ethische normen of overeenkomsten die van toepassing zijn op de activiteiten van de Klant. De Klant erkent dat de toepasselijke wetgeving onderhevig kan zijn aan wijzigingen, en stemt er mee in om deze wijzigingen nauwkeurig op te volgen en zich hierover te laten adviseren door zijn eigen adviseurs.

CBC zal alles in het werk stellen om de continuïteit van de Business Dashboard Security te verzekeren. CBC kan zevenwel niet aansprakelijk worden gesteld wanneer het Dashboard of bepaalde Diensten tijdelijk niet beschikbaar zijn door geplande onderhoudswerkzaamheden, of niet-geplande onderhoudswerkzaamheden die een redelijke duur niet overschrijden of door Overmacht. CBC zal de Klant(en) tijdig op de hoogte brengen van een onbeschikbaarheid ingevolge geplande onderhoudswerkzaamheden en de vermoedelijke duur ervan.

2.7 Wijzigingen aan deze Business Dashboard Overeenkomst – Voorwaarden Beveiliging

CBC behoudt zich het recht voor om de bepalingen van deze Business Dashboard Overeenkomst – Voorwaarden Beveiliging te wijzigen. Iedere wijziging wordt een redelijke termijn vóór de datum van de beoogde inwerkingtreding aan de Klant meegedeeld met een bericht in de Digitale toepassing, of op een andere voor de Klant toegankelijke drager. De Klant beschikt over de mogelijkheid om binnen de kennisgevingstermijn de overeenkomst onmiddellijk en kosteloos op te zeggen wanneer hij niet akkoord gaat met de voorgestelde wijzigingen. Wijzigingen worden voor de Klant bindend wanneer hij de overeenkomst niet heeft opgezegd binnen voormelde termijn.

3 CBC-eBusinesskaart

De specifieke veiligheidsregels van de CBC-eBusinesskaart en het bijhorend Digitaal certificaat zijn vastgelegd in de Certificate Policy. Bijkomend moeten de Klant en de Gebruikers volgende veiligheidsregels naleven:

3.1 Veilige configuratie van de computer

De Gebruiker mag enkel gebruik maken van software die door een officiële distributeur erkend is en moet de richtlijnen van de distributeur strikt volgen.

3.2 De installatie van de CBC beveiligingssoftware op de computer

De Gebruiker dient de CBC beveiligingssoftware, die instaat voor het correct gebruik van de CBC-eBusinesskaart op zijn computer te installeren en actief te laten gedurende het gebruik van de Digitale toepassing(en).

Bijkomend biedt CBC een software aan die zich specifiek richt op het detecteren en neutraliseren van computervirussen die een bedreiging vormen voor de Digitale toepassing(en). Deze software biedt een extra beveiliging voor de browser-toepassing (een programma met een grafische gebruikersinterface voor het weergeven van HTML bestanden die het mogelijk maakt op het World Wide Web te navigeren) bij het connecteren met de Digitale toepassing(en). Meer informatie over de CBC beveiligingssoftware is terug te vinden op https://entreprendre.cbc.be/exigencestechniques.

3.3 De CBC-eBusinesskaart verwijderen uit de kaartlezer

De gebruiker dient zijn smartcard steeds te verwijderen uit de CCR wanneer hij geen actief gebruik maakt van de Digitale toepassing.

4 eBusiness Portal Kaart

4.1 Registratie en certificatie - Algemeen

De eBusiness Portal Kaart vereist voorafgaande registratie bij de RA en de uitgifte van één of meer certificaten door de CA. Deze registratie- en certificatiediensten worden verleend overeenkomstig de voorwaarden van de toepasselijke CP. De CP legt onder meer de rechten en plichten van de Partijen vast met betrekking tot het registratie- en certificatieproces, de gebruiksvoorwaarden, de periode waarvoor de gegevens worden opgeslagen en de procedure voor herroeping van certificaten. De Klant verplicht zich tot naleving van de CP.

4.2 Registratie

Registratie vereist de indiening door de Klant van de door de RA gevraagde gegevens en documenten, waaronder identiteit, handelingsbekwaamheid en overige specifieke eigenschappen en bevoegdheden. Ten behoeve van de uitgifte van het Certificaat dient bovendien iedere Gebruiker van het eBusiness Portal Kaart op de juiste manier geregistreerd te worden conform de CP ("Gebruiker(s)"). De door de RA gevraagde gegevens dienen voor iedere Gebruiker verstrekt te worden en iedere Gebruiker die een natuurlijk persoon is dient in te stemmen met deze Algemene Voorwaarden zoals deze gelden ten aanzien van Klanten.

De Klant garandeert dat alle verstrekte gegevens en/of documenten, met inbegrip van de gegevens van de Gebruikers indien van toepassing, correct zijn.

De Klant erkent en aanvaardt dat de RA geen enkele verantwoordelijkheid draagt tegenover de Klant in verband met de verificatie van de door de Klant verstrekte gegevens. Conform de bepalingen van de CP, zal de Klant de RA onverwijld in kennis stellen van elke wijziging in de gegevens en documenten die door de Klant zijn verstrekt. De Klant is aansprakelijk voor alle schade die veroorzaakt kan worden door de verstrekking van onjuiste of onvolledige gegevens en/of documenten. De RA verbindt zich ertoe om wijzigingen in de gegevens die aan haar verstrekt zijn door de Klant en Gebruikers zo spoedig mogelijk te verwerken, in overeenstemming met de daarvoor bestemde procedures die in de CP zijn vastgelegd.

4.3 Uitgifte van een Certificaat

De CA zal één of meer Certificaten uitgeven aan Gebruikers die door de RA aanvaard zijn en die de registratieprocedure zoals vastgelegd in de CP doorlopen hebben. De CA behoudt zich het recht voor om uitgifte van een Certificaat te weigeren ingevolge de toepasselijke wetgeving op elektronische handtekeningen en de CP. De Klant verbindt zich ertoe om die Gebruikers die natuurlijke personen zijn op de hoogte te stellen van alle verplichtingen die de Klant is aangegaan in het kader van deze Overeenkomst. De Klant waarborgt dat Gebruikers deze verplichtingen zullen naleven. Ieder gebruik van eBusiness Portal Kaart door een Gebruiker zal worden geacht afkomstig te zijn van de Klant. De eBusiness Portal Kaart stelt de Gebruiker in staat om, met behulp van de gegevens waarmee een handtekening kan worden aangemaakt en gewaarborgd door een Certificaat, zichzelf te authenticeren en een elektronische handtekening onder berichten te plaatsen. Deze elektronische handtekening mag uitsluitend worden gebruikt binnen het kader dat vastgelegd is in deze Algemene Voorwaarden.

Certificaten worden uitgegeven voor een in de CP bepaalde periode.

4.4 Herroeping van het Certificaat

De Klant verklaart de voorwaarden voor herroeping, de procedure inzake een herroepingsverzoek, evenals de overige bepalingen van de CP inzake de herroeping van een Certificaat te kennen, te aanvaarden en te respecteren.

5 CBC Sign

5.1 Eerste gebruik en personaliseren van CBC Sign

De Gebruiker kan via de applicatiewinkel de CBC Sign app downloaden en installeren op zijn Toestel. Hij kan CBC Sign maar op één toestel registreren. Als de Gebruiker CBC Sign registreert op een tweede Toestel, wordt CBC Sign op het eerste Toestel gedesactiveerd. De gebruiker kan CBC Sign herinstalleren wegens veranderen van toestel of technische problemen en het verwijderen van de applicatie.

Elke Gebruiker dient bij de registratie van CBC Sign in te stemmen met het Reglement CBC-Sign. Dit reglement is van toepassing op alle Gebruikers, behoudens Gebruikers die zelf geen CBC-klant zijn en slechts op afstand werden geïdentificeerd door de Klant (hierna de CBC Sign Light Gebruikers genoemd). De Klant moet voor elke CBC Sign Light Gebruiker beschikken over een akkoordverklaring met de bepalingen van deze Business Dashboard Overeenkomst – Voorwaarden Beveiliging en zijn Bijlagen. De CBC Mobile Sign Light Gebruikers kunnen CBC Sign enkel gebruiken als Toegangs- en ondertekeningsmiddel voor die Digitale toepassing waarvoor zij expliciet door de Klant gemachtigd zijn.

De registratie en personalisatie van CBC Sign kan gebeuren op de volgende wijzen:

5.1.1 De Gebruiker gebruikt CBC Sign enkel als Gebruiker in de Digitale toepassing van de Klant.

De Klant zal de Gebruiker registreren voor het gebruik van CBC Sign, hetzij via de Digitale toepassing, indien mogelijk, hetzij via zijn kantoor, of zijn verzekeringsagent als hij alleen verzekeringsklant is. Tenzij de Gebruiker CBC Sign al gebruikt voor zijn eigen digitale toepassingen, en de CBC Sign app zelf kan activeren met ofwel met zijn Kaart, bijhorende pincode en Kaartlezer ofwel via zijn CBC-Mobile app zoals hierna uiteengezet onder punt (2), ontvangt de Gebruiker een eenmalig te gebruiken user-ID en QR-code. Dit laatste zal steeds het geval zijn voor de CBC Sign Light Gebruiker. De Gebruiker kan de user-ID afhalen in het kantoor of bij de verzekeringsagent of wordt hem ter beschikking gesteld door de Beheerder van de Digitale toepassing. De QR-code wordt elke Gebruiker persoonlijk toegestuurd per post, e-mail of via de rapportentoepassing van zijn Digitale toepassing. Als de Gebruiker zelf beschikt over een Kaart, kan hij via de CBC-non-cashautomaten zijn user-ID en de QR-code opvragen. User-ID en QR-code zijn vertrouwelijk en hebben slechts een beperkte geldigheidsduur, die wordt meegedeeld via en bepaald afhankelijk van het gekozen verzendingskanaal.

Bij het eerste gebruik van de CBC Sign app moet de Gebruiker zijn user-ID ingeven en vervolgens de QR-code scannen met zijn Toestel. Op basis van de user-ID en QR-code wordt een registratieproces uitgevoerd en wordt een geheime sleutel aangemaakt op zijn Toestel. Die geheime sleutel wordt verbonden met de specifieke Gebruiker en met zijn Toestel. Vervolgens moet de Gebruiker een Geheime code kiezen, bestaande uit 5 cijfers. Die Geheime code dient om de Gebruiker te identificeren en om de geheime sleutel op zijn Toestel te beveiligen. De Geheime code wordt nergens opgeslagen, ook niet aan CBC-zijde.

5.1.2. De Gebruiker gebruikt CBC Sign ook voor zijn eigen (privé) digitale toepassing

Een Gebruiker die CBC Sign ook gebruikt voor zijn eigen digitale toepassingen kan zich authentiseren en registreren voor het gebruik van CBC Sign en de CBC Sign app activeren (1) met zijn Kaart, bijhorende pincode en Kaartlezer, of (2) via de CBC-Mobile app.

Tijdens het registratieproces wordt een geheime sleutel aangemaakt die wordt verbonden met de Gebruiker en met zijn Toestel. Vervolgens moet de Gebruiker een Geheime code kiezen, bestaande uit 5 cijfers. Die Geheime code dient om de Gebruiker te identificeren en om de geheime sleutel op zijn toestel te beveiligen. De Geheime code wordt nergens opgeslagen, ook niet aan CBC-zijde.

5.2 Aanmelden met CBC Sign

Bij het aanmelden (toegangscontrole) gebruikt de Gebruiker zijn login-ID om zich te identificeren in de Digitale toepassing. De web toepassing genereert vervolgens een unieke en beveiligde QR-code. In het startscherm van de CBC Sign app kiest de Gebruiker voor aanmelden en scant hij de QR-code. Vervolgens voert de Gebruiker zijn Geheime code in de CBC Sign app. Indien de Geheime code correct is krijgt de Gebruiker toegang tot de digitale toepassing op zijn computer.

5.3 Opdrachten ondertekenen met CBC Sign

Door te klikken op de teken-knop in de Digitale toepassing ontvangt de Gebruiker een overzicht van de te ondertekenen Opdracht(en) in het 'tekenscherm' van de CBC Sign app. Na validatie van de inhoud kan de Gebruiker de Opdracht(en) ondertekenen in CBC Sign door zijn Geheime code in te voeren. Indien de Geheime code correct is wordt(en) de Opdracht(en) als getekend weergegeven in de Digitale toepassing.

5.4 Reset van de Geheime code

Wanneer de Gebruiker drie (3) maal een verkeerde Geheime code ingeeft wordt CBC Sign geblokkeerd. Als de Gebruiker beschikt over een eigen Kaart en Kaartlezer, kan hij vanop afstand zijn Toestel deblokkeren en een nieuwe Geheime code kiezen.

De gebruiker kan aan de Beheerder vragen om geheime code te resetten zodat de gebruiker deze zelf kan terug her instellen.

Als de Gebruiker niet over een eigen kaart of kaartlezer beschikt en CBC Sign alleen gebruikt voor de Digitale toepassing van de Klant en geen Beheerder is van het Business Dashboard, moet de Gebruiker de helpdesk (https://www.cbc.be/entreprendre/fr/contact.) contacteren.

5.5 Nieuwe versies van de CBC Sign-app

CBC investeert in technologische ontwikkelingen en in de veiligheid van CBC Sign. Daarom zal CBC regelmatig nieuwe versies van CBC Sign uitbrengen (hierna 'updates'). De Gebruiker zal in de applicatiewinkel op zijn Toestel een melding krijgen van die updates en een samenvatting van de voornaamste wijzigingen.

De goede werking en veiligheid van CBC Sign kan maar gegarandeerd worden als de Gebruiker altijd beschikt over de meest recente versie van de CBC Sign app. De Gebruiker moet elke nieuwe update zo snel mogelijk installeren zodra deze wordt aangeboden. Zodra de Gebruiker de update versie geïnstalleerd heeft, kan de Gebruiker de vorige versie van CBC Sign niet meer gebruiken.

5.6 Specifieke vereisten inzake beveiliging

5.6.1 Veilige configuratie van het mobiel Toestel met de app CBC Sign

De Gebruiker verbindt zich ertoe:

- enkel gebruik te maken van software die door een officiële distributeur erkend is, en daarbij strikt de richtlijnen van de distributeur te volgen. Er mag geen gebruik gemaakt worden van illegale software;
- een schermbeveiliging (zoals een toegangscode) te activeren op zijn Toestel.

CBC kan de installatie en het gebruik van de CBC Sign app op bepaalde toestellen verhinderen om objectief gerechtvaardigde redenen die verband houden met de veiligheid van de Digitale toepassing en/of van CBC Sign. Dit is het geval bij mobiele toestellen voorwerp van een Jailbreak of Rooting.

5.6.2 De Geheime code van de CBC Sign app

De Gebruiker verbindt zich ertoe om steeds waakzaam om te gaan met de CBC Sign Geheime code, en om:

- de Geheime code nooit aan anderen te laten zien of mee te delen (met inbegrip van partner, familie en vrienden);
- de Geheime code discreet in te voeren en ervoor te zorgen dat niemand kan meekijken als hij de code invoert;
- elk vastgesteld ongewoon gedrag te melden aan CBC;
- de Geheime code niet via het klavier van de computer in te voeren;
- de Geheime code niet op het Toestel te noteren of te kleven;
- een Geheime code te kiezen die niet gemakkelijk te raden is (dus best geen verjaardag of geboortejaar, eigen postcode, enz.);
- wanneer men de Gebruiker ernaar vraagt, bijvoorbeeld telefonisch of per e-mail, op een website of in een app anders dan de CBC Sign app, deze nooit mee delen. CBC-medewerkers vragen nooit codes aan de Gebruikers.

5.6.3 Verificatie van de Opdrachten op het scherm van het mobiel Toestel

De Gebruiker moet steeds de Opdrachten geïnitieerd via de Digitale toepassing verifiëren alvorens ze te bevestigen met zijn Geheime code.

De Gebruiker moet elk verlies of diefstal van zijn Toestel en/of Geheime code onverwijld melden zoals bepaald in artikel 2.5.3.