Business Dashboard Agreement
Security Conditions

These regulations were registered in Leuven on on 22 February 2018 and are effective from on 26 February 2018 until further notice. This publication contains 6 pages.

1 Definitions

Except where expressly stipulated otherwise, the definitions from the Business Dashboard Agreement – General Provisions also apply in these Business Dashboard Agreement – Security Conditions. The definitions may be used without distinction in the singular or plural form.

Access Code

The personal, confidential identification code that the User must enter in CBC Sign to identify that User or to sign Orders/Instructions.

Agreement

The Agreement comprises:

- the Application Form;
- the Business Dashboard Agreement – General Provisions;
- the Application Contracts;
- the Business Dashboard Agreement – Special Provisions;
- the Business Dashboard Agreement – Security Conditions;
- the Documentation and the Annexes;

and all amendments and additions that may be agreed in writing between the Parties at a later time.

Application Form

The part of the Business Dashboard Agreement which is signed by the Customer(s) and which identifies the contracting parties, the specific Services received and the applicable contractual conditions.

Annexes

Documents which the Parties agree will be attached to these Business Dashboard Agreement – Security Conditions. All Annexes are subject to these Business Dashboard Agreement – Security Conditions.

Authentication

The method by which the identity is reliably established.

Business Dashboard Security

The Means of Access and Signature which enable the User to secure authentication and place an electronic signature. This electronic signature may only be used within the context of the Digital Applications and, under certain conditions, for e-Government applications in Belgium. The Business Dashboard Security enables the User(s):

i. To access the Digital Applications as indicated on the Application Form;

ii. To initiate and confirm Orders/Instructions and, under certain conditions, to use e-Government applications.

Card

The CBC Bank Card that a User holds and uses together with the related PIN and Card Reader to log in to certain Digital Applications. Use of the Card is governed by the CBC Bank Card Regulations.

Card Reader

A device that, in combination with the Card and PIN associated with the Card, generates new codes that Users can use to log in and sign Orders/Instructions in certain Digital Applications.

Certificate

A Digital Certificate issued by the CA.

Certification Authority or CA

The authority responsible for certification. At the time of signing this Agreement, Isabel NV, with registered office at Keizerinlaan 13-15, 1000 Brussels, Belgium, is responsible for the issuing and administration of Certificates. The certification services are provided in accordance with this Agreement and the terms and conditions of the applicable Certificate Policy, as defined below.

Certificate Policy or CP

The PKI@CBC Certificate Policy which sets out rules in respect of the applicability of a Certificate to a particular community and/or class of application with common security requirements. The full text of the CP can be found on the following website: www.kbc.com/certificate-policy. The Certificate Policy mainly sets out the basic obligations of the CA and the other parties involved in CBC's Public Key Infrastructure (PKI). The PKI is a system allowing Digital Certificates to be issued and managed.

Certificate Revocation List

A list of revoked Certificates which have been digitally signed by the issuing CA.

Connected Card Reader or CCR

The Card Reader that is connected to the User's computer and that is used to read a smart card, such as the CBC eBusiness Card or the CBC eBusiness Portal Card.

Device

A smartphone onto which the CBC Sign app can be downloaded. The requirements that the Device must meet are set out at www.cbc.be/sign et https://entreprendre.cbc.be/exigencestechniques.

Digital Applications

The Services and Dashboard Functionalities located behind the Dashboard and forming part of the Business Dashboard Agreement, for which the Customer(s) and/or the User(s) use the Business Dashboard Security.

Digital Certificate

A computer file containing the Certificate-holding User's Public Key, identity and other information (such as the validity of the Certificate, the identity of the issuer, the location of the Certificate Revocation List) and a summary of the aforementioned details reduced to a unique code and encrypted using the Private Key of the Certification Authority (CA).

The Digital Certificate is issued and managed by the CA. The CA guarantees the integrity and authenticity of the Digital Certificate.

Documentation

The documentation appended to or referred to in the Business Dashboard Agreement – Security Conditions, such as the CP.

eBusiness Portal Card

A smart card which stores the Private Key of the certified User and is used by the certified User to create an electronic signature.

Jailbreak/Rooting

An action enabling circumvention of a Device's security (jailbreaking applying to iPhones and rooting applying to Android or other smartphones) and allowing software to be loaded onto it that is not recognised or approved by the device's official distributor. As a result, Devices are more susceptible to viruses and malware (software designed to harm or disable computers and computer systems).

CBC

The Bank, the Insurer or the entity forming part of the KBC Group which acts as the distributor of the Digital Application and the Business Dashboard Security.

CBC eBusiness Card

A smart card incorporating a Private Key that generates a digital signature, with which the User (i) logs in to the Dashboard and the Digital Application(s) and (ii) can sign Orders/Instructions. A Certificate issued along with the CBC EBusiness Card confirms that the signatory User is the holder of a Private and a Public Key.
Each message or Order/Instruction to be signed is reduced to a unique code, which is encrypted using the User's Private Key and can only be verified using the User's Public Key. The Public Key can be retrieved by anyone.

CBC Mobile App

The set of procedures agreed between the User and the Bank that provide access to the services of CBC Mobile Banking on the User's own Device and enable the User to use mobile banking.

CBC Sign

The Means of Access and Signature Tool that enables a User, via the CBC Sign app installed on a mobile Device (smartphone), and separately from the Digital Application, to:

i. be authenticated (verification that the User is in fact who they say they are);
ii. sign Orders/Instructions in the Digital Application.

Means of Access and Signature

The required means by which a User (i) is authenticated and given access to the Digital Application; and (ii) is able to sign Orders in the Digital Application, and for which that User has either entered into a contract with CBC itself or has been designated as an authorised User by the Customer. An overview of these Digital Applications can be viewed at www.cbc.be/sign and on the Application Form.

Order/Instruction

An Order or Instruction initiated by a User including, but not limited to, payment or investment transactions and any instructions by which they enter into a new or amended contract with CBC.

Party and Parties

The Customer(s) or CBC, designated individually as Party and jointly as Parties.

Private Key

The key that is known only to the User and is used to encode (encrypt) or sign information.

Public Key

The key that is public and is used to decode (or decrypt) the information again or to verify a User's identity.

QR-code

A two-dimensional barcode allowing the fast, user-friendly transfer and scanning of (digital) information.

Registration Authority (RA))

The Bank and/or the Insurer, or any other entity forming part of the KBC Group which determines which User(s) may be issued with a Digital Certificate, and which is responsible for the identification and registration of that (those) User(s). The RA does not sign or issue Certificates. The RA may assist in the Certificate application and/or revocation process, in accordance with the provisions of the applicable CP.

User

A natural person or a department of a Customer, duly identified and authorised to use Services and Dashboard Functionalities designated for that Customer within the Agreement in the name and for the account of that Customer and within the scope of this Agreement. A User who has been identified remotely by a Customer, and who is themselves not a fully identified CBC Customer, will also be designated as a CBC Sign Light User for the use of CBC Sign.

2 General Provisions

2.1 General

These Business Dashboard Agreement – Security Conditions form part of the Security Terms & Conditions in the General Provisions of the Agreement and set out the rights and obligations of CBC, the Customer(s) and the User(s), respectively, in relation to the use of the Business Dashboard Security.

2.2 Liability of Parties

The Parties acknowledge that the liability clauses, and specifically the liability limitations as set out in the Agreement, are applicable to the Business Dashboard Security.

2.3 Intellectual Property Rights

CBC or its third-party licensors is (are) and remain(s) the owner of the Intellectual Property Rights and know-how associated with the Business Dashboard Security. No rights are attributed to the Customer(s) and/or the User(s) other than those expressly stated in the Agreement.

In so far as CBC makes software or Documentation available in the context of the provision of Business Dashboard Security, CBC grants the Customer(s) for each User a non-transferable, limited, non-exclusive license to use the Business Dashboard Security. This usage is restricted to the Customer's/ Customers' own business purposes. The Customer(s) must take all necessary measures to safeguard the KBC Group entity's Intellectual Property Rights associated with the Business Dashboard Security.

In the event of a complaint from a third party in connection with a breach by CBC of the Intellectual Property Rights of third parties, the Customer(s) undertake(s) to inform CBC immediately of such complaint, as well as to provide all information and support, and to grant CBC the right to conduct any legal proceedings and negotiations. In the event that CBC deems that a program may have breached the Intellectual Property Rights of a third party, CBC will at its sole discretion choose to adapt the program in breach in such a way that there is no longer a breach, or to obtain the right on behalf of the Customer(s) to continue using the program, or, should CBC be of the opinion that neither of those options can be achieved, to terminate the right of use for the program in question and to reimburse any fees paid by the Customer(s) for that program.

2.4 Electronic signature, evidence and notification

The Parties agree that the electronic signature created by a User using the appropriate procedures is equivalent to a handwritten signature and meets the requirements of Article 1322, paragraph 2 of the Belgian Civil Code. This applies to the relationship between CBC and the Customer(s).

The Parties also agree that the electronic signature in all cases has all legal consequences ascribed by the law vis-à-vis CBC, its Customers and third parties.

Electronic messages, connections, transactions between the Customer(s) and CBC will be proven using the logs and transaction files kept electronically by CBC. The Customer(s) accept(s) the evidential value of this data. This method of providing proof does not prevent the Parties from each providing their own proof using permitted legal methods.

CBC records access to the Digital Applications by means of the Business Dashboard Security. CBC maintains a log in which it only stores data relating to the use of the Business Dashboard Security. This log can be reproduced on paper or any other type of information medium. It provides evidence that access has been gained to the Digital Applications, unless the Customer(s) can provide evidence to the contrary.

2.5 Obligations of the Customer(s)

2.5.1. General

The Customer(s) will ensure that the Business Dashboard Security is used in accordance with these General Terms and Conditions, the Technical Requirements, national and international legislation and, in general, in a responsible manner, exclusively for admissible purposes and without breaching the rights of third parties.

CBC will advise the Customer(s) and the User(s) of the security instructions and the measures to be taken when using the Dashboard and the underlying Digital Applications through these Business Dashboard Agreement – Security Conditions, the Special Provisions applying to the Digital Applications and the webpages referred to in Article 2.6. The Customer(s) and the User(s) are expected to consult these webpages regularly, and at least once per month.

Neither the Customer(s) nor the User(s) are permitted to make modifications to the Business Dashboard Security. The Customer(s) is (are) liable for all damage that may ensue from modifications made, or from the improper or incorrect use thereof by the Customer(s) or its (their) User(s). The Business Dashboard Security will be installed by the Customer(s). Under no circumstances will CBC be held liable for the consequences of an error or omission that may occur during this installation by the Customer(s) or by a third party.

2.5.2. Customer equipment

The Customer(s) undertake(s) only to use hardware and software which meets the Technical Requirements as notified to the Customer(s) by CBC and which are necessary for the use of the Business Dashboard Security. CBC reserves the right to amend these Technical Requirements from time to time.

All costs of purchasing, installing and operating the Business Dashboard Security will be borne by the Customer(s).

2.5.3. Security and management of the Means of Access and Signature

Unless expressly stipulated otherwise in the Special Provisions, the Means of Access and Signature are strictly personal. The Customer(s) is (are) responsible for the safeguarding, confidentiality, security and appropriate use of the Means of Access and Signature by the Customer(s) and its (their) User(s) and undertake(s) to take all requisite steps to prevent any unauthorised third party from being able to gain knowledge or make use thereof.

In the event of loss, theft, breach of confidentiality or any risk of abuse of the Means of Access and Signature, or in the event of loss or theft of its Device, the Customer(s) and the User(s), respectively, must notify the following organisations immediately:

- CBC on telephone number 0800 65 650;
- the RA in the event of use of the eBusiness Card or the CBC eBusiness Portal Card as stipulated in the respective CPs.

It is also advisable for the Customer(s) and/or the User(s) to report the matter to the police.

The Customer(s) is (are) fully and unconditionally responsible for any use of the Digital Applications, as well as for any detrimental consequences that may arise directly or indirectly therefrom, until the time that such notification is made.

Other than in the event of actual or attempted fraud, wilful act or gross misconduct, the Customer(s) is (are) no longer liable for any further loss or damage after such notification has been made.

In the event that CBC has any reason to suspect a breach of the confidentiality and/or security of the Means of Access and Signature, or abuse of the Digital Applications, it may suspend access to the Digital Applications.

In the event that a Customer uses the Means of Access and Signature by making use of a Certificate, that Customer must in the event of theft, loss or any other established abuse of the Certificate, or any doubts in this regard, or in the event that the information on the Certificate is no longer current, revoke the Certificate in accordance with the procedure as set out in the CP. The Customer(s) is (are) responsible for all damage that may be suffered by the Customer itself, CBC or third parties as a result of non-revocation or late revocation.

2.6 CBC's obligations

CBC undertakes to exercise all due care in the performance of this Agreement. CBC will take the requisite steps to ensure the continuity of the Business Dashboard Security. CBC cannot guarantee that the Business Dashboard Security will meet the specific expectations, objectives or requirements of the Customer(s) or User(s).

CBC will advise the Customer(s) and the User(s) of the security instructions and the measures to be taken when using the Dashboard and the underlying Digital Applications through these Business Dashboard Agreement – Security Conditions, the Special Provisions applying to the Digital Applications and the following webpages:

- Urgent security notifications on the login pages of the Dashboard: https://entreprendre.cbc.be en www.cbccorporate.be
- General security awareness and specific security tips: https://secure4u.cbc.be/
- Specific security requirements with regard to users' infrastructure (as part of the system requirements): https://entreprendre.cbc.be/exigencestechniques

The Customer(s) alone, and not CBC under any circumstances, is (are) required to check that the use of Business Dashboard Security by the Customer complies with all legislation, regulations, ethical rules or agreements that apply to its activities. The Customer(s) acknowledge(s) that the applicable legislation may be subject to change, and agree(s) to adhere strictly to any such changes and to seek advice from its (their) own advisers on this.

CBC will do everything possible to ensure the continuity of the Business Dashboard Security. CBC can however not be held liable in the event that the Dashboard or certain Services are temporarily unavailable due to planned or unplanned maintenance work which does not exceed a reasonable duration, or due to Force Majeure. CBC will advise the Customer(s) in good time of any unavailability due to planned maintenance work and its likely duration.

2.7 Amendments to these Business Dashboard Agreement – Security Conditions

CBC reserves the right to amend the provisions of these Business Dashboard Agreement – Security Conditions. The Customer(s) will be given a reasonable amount of notice before the date that an amendment is scheduled to take effect, by means of a message in the Digital Application or on another medium to which the Customer(s) has (have) access. The Customer(s) may avail itself (themselves) of the opportunity within that period to terminate the agreement forthwith and at no cost if it (they) do(es) not agree to the proposed amendments. Amendments will be binding on the Customer(s) if it (they) do(es) not terminate the contract within the said period.

3 CBC eBusiness Card

The specific security rules for the CBC eBusiness Card and the associated Digital Certificate are laid down in the Certificate Policy. In addition, the Customer(s) and the User(s) must comply with the following security rules:

3.1 Secure configuration of computers

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 Installing CBC security software on computers

Users must install CBC's security software (which ensures proper use of the CBC EBusiness Card) on their computer and make sure it is kept active whenever using the Digital Application(s).

In addition, CBC offers software specifically designed to detect and neutralise computer viruses that pose a threat to the Digital Application(s). This software offers extra security for browser applications (programs with a graphic user interface for displaying HTML files, thus allowing users to navigate around the World Wide Web) when connecting to the Digital Application(s)

More information about CBC's security software may be found at https://entreprendre.cbc.be/exigencestechniques.

3.3 Removing the CBC eBusiness Card from the Card Reader

Users must always remember to remove their smart card from their CCR when not actively using the Digital Application.

4 eBusiness Portal Card

4.1 Registration and certification – General

Before it can be used, the eBusiness Portal Card must be registered with the RA and one or more certificates must be issued by the CA.

These registration and certification services will be provided in accordance with the terms and conditions of the applicable CP. Among other things, the CP lays down the rights and obligations of the parties in relation to the registration and certification process, the conditions governing use, the period for which data is stored and the procedure used to revoke certificates. The Customer(s) undertake(s) to comply with the CP.

4.2 Registration

Registration requires the submission by the Customer(s) of the information and documents requested by the RA, including identity, legal authority and other specific capacities and powers. In addition, for the purpose of issuing the Certificate, all Users of the eBusiness Portal Card must be duly registered in accordance with the CP ('User(s)'). The information requested by the RA must be provided for every User, and any User who is a natural person must agree with these Terms and Conditions, as applied to Customers.

The Customer(s) guarantee(s) that all information and/or documents provided, and where applicable those of the User(s), are correct.

The Customer(s) acknowledge(s) and accept(s) that the RA bears no liability whatsoever towards the Customer(s) regarding verification of the information provided by the Customer(s). In accordance with the terms and conditions of the CP, the Customer(s) will notify the RA forthwith of any change to the information and documents provided by the Customer(s). The Customer(s) is (are) liable for any damage that may be caused by the provision of incorrect or incomplete information and/or documents. The RA undertakes to assimilate as quickly as possible any change to the information provided to it by the Customer(s) and the User(s), in accordance with the appropriate procedures laid down in the CP.

4.3 Issue of a Certificate

The CA will issue one or more Certificate(s) to User(s) accepted by the RA who have completed the registration procedure laid down in the CP. The CA reserves the right to refuse to issue a Certificate pursuant to the applicable legislation on electronic signature and the CP. The Customer(s) undertake(s) to inform those of its Users who are natural persons of any and all commitments that the Customer(s) has (have) entered into under this Agreement and will ensure that the User(s) observe(s) these commitments. Any use of the eBusiness Portal Card by a User will be considered as emanating from the Customer. The eBusiness Portal Card enables the User, using the information with which a signature can be created and guaranteed by a Certificate, to authenticate itself and to append an electronic signature at the end of messages. This electronic signature may only be used in the context laid down in these General Terms & Conditions.

Certificates are issued for a period defined in the CP

4.4 Revocation of the Certificate

The Customer(s) declare(s) that it (they) is (are) aware of, accept(s) and will comply with the circumstances for revocation, the procedure for a revocation request and other clauses concerning the revocation of a Certificate mentioned in the CP.

5 CBC Sign

5.1 First use and personalisation of CBC Sign

Users can download the CBC Sign App from the app store and install it on their Device. Each User can only register CBC Sign once. If a User registers CBC Sign on a second Device, CBC Sign will be deactivated on that User's first Device. Users can reinstall KBC Sign if they change their device or experience technical issues and have first uninstalled the application. When registering, each User is required to agree to the CBC Mobile Sign Regulations. These Regulations apply to all Users, except Users who are themselves not CBC Customers and have only been identified remotely by the Customer(s) (referred to hereinafter as CBC Sign Light Users). For every CBC Sign Light User, the Customer(s) must be in possession of a declaration of agreement with the provisions of these Business Dashboard Agreement – Security Conditions plus Annexes. CBC Mobile Sign Light Users may only use CBC Mobile Sign as a Means of Access and Signature Tool for the Digital Application for which they have been explicitly authorised by the Customer(s). CBC Sign can be registered and personalised as follows:

5.1.1 The User uses CBC Sign only as a User in the Digital Application of the Customer.

The Customer will register the User to use CBC Sign, either via the Digital Application, if possible, or at their branch (or insurance agent if they are an insurance Customer only). Unless the User already uses CBC Sign for their own Digital Applications and can themselves activate the CBC Sign app either using their Card, associated PIN and Card Reader or using their CBC Mobile Banking app as explained below under (2), the User will receive a single-use user ID and QR code. This will be the case at all times for CBC Sign Light Users. Users can collect the user ID from their branch or insurance agency or one will be provided to them by the Administrator of the Digital Application. The QR code is sent to each User personally by post or e-mail or via the reports feature of the User's Digital Application. If Users themselves possess a Card, they can obtain their user ID and QR code at any non-cash CBC ATM. The user ID and QR code are confidential and have limited validity, notified via and set depending on the manner chosen to receive communications.

When first using the CBC Sign app, the User must enter their user ID and then scan the QR code using their Device. The user ID and QR code trigger a registration process, and a secret key is generated on their Device, which is then linked with that specific User and with that Device. The User must then create a five-digit Secret Code, which is used to identify the User and secure the Secret Key on the User's Device. The Secret Code is not stored anywhere, including at CBC.

5.1.2. Users that also use CBC Sign for their own (personal) Digital Application

Users that also use CBC Sign for their own Digital Applications can authenticate and register themselves to use CBC Sign and activate the CBC Sign app (1) using their Card, associated PIN and Card Reader or (2) via the CBC Mobile Banking app.

During the registration process, a secret key is generated that is linked to the User and to his/her device. The User must then create a five-digit Secret Code, which is used to identify the User and secure the Secret Key on the User's Device. The Secret Code is not stored anywhere, including at CBC.

5.2 Logging in with CBC Sign

When logging in (access control), Users use their login ID to identify themselves in the Digital Application. The browser application then generates a unique, secure QR code. When the CBC Mobile app start screen appears, the User selects 'Log in' and scans the QR code. The User then enters their Secret Code in the CBC Sign app. Provided the Secret Code is correct, the User then gains access to the Digital Application on their computer.

5.3 Signing Orders/Instructions using CBC Sign

Clicking on the 'Sign' button in the Digital Application gives the User an overview of Orders/Instructions to be signed in the CBC Sign app's 'signature screen'. After validating the content, the User can sign Orders/Instructions in CBC Sign by entering their Secret Code. If the Secret Code is correct, each Order/Instruction is shown as signed in the Digital Application.

5.4 Resetting the Secret Code

If a User enters the Secret Code incorrectly three times in a row, CBC Sign will be blocked. If a User has their own Card and Card Reader, he/she can unblock their Device remotely and select a new Secret Code.

Users can ask the administrator to reset the PIN so that they can reinstall it themselves.

Users that have no card or card reader of their own and only use KBC Sign for the Client's Digital application and are not Business Dashboard Administrators, must contact the Helpdesk (https://www.cbc.be/entreprendre/fr/contact.).

5.5 New versions of the CBC Sign app

CBC is constantly investing in developing the CBC Sign technology and security and will therefore regularly issue new versions of CBC Sign ('updates'). Users will be notified on their Device when updates are available from their app store, and will also receive a summary of the main changes.

The proper functioning and security of CBC Sign can only be guaranteed if Users always have the most recent version of the CBC Sign app. Users must install each update as soon as possible after it is offered to them. Once Users have installed the update version, they can no longer use the previous version of CBC Sign.

5.6 Specific security requirements

5.6.1 Secure configuration of the mobile Device with the CBC Sign app

The User(s) undertake(s):

- Only to use software that is recognised by an official distributor and to adhere strictly to the distributor's guidelines. No use may be made of illegal software.
- To activate a screen lock (such as an access code) on their Device.

CBC can prevent installation and use of the CBC Sign app on certain devices for objectively justified reasons relating to the security of the Digital Application and/or CBC Sign. This applies to mobile devices that have been subject to Jailbreaking or Rooting.

5.6.2 The Secret Code for the CBC Sign app

Users undertake to take care of the CBC Sign Secret Code and:

- ever to show or divulge the Secret Code to other persons (including partner, family and friends);
- to enter the Secret Code discreetly and ensure that no one can observe them as they do so;
- to notify CBC if they notice any unusual behavior;
- not to enter the Secret Code using a computer keyboard;
- not to write down or affix the Secret Code on the Device;
- to choose a Secret Code that cannot easily be guessed (e.g. not using a birthday or year of birth, own postcode, etc.);
- never to divulge the Secret Code to anyone who asks them for it, such as by telephone or e-mail, on a website or in an app other than the CBC Sign app. CBC staff will never ask Users for their codes.

5.6.3 Verifying Orders/Instructions on the mobile Device screen

Users must always check Orders/Instructions initiated using the Digital Application before confirming them using their Secret Code.

5.6.4 Reporting loss or theft

Users must report every loss or theft of their Device and/or Secret Code immediately in the manner described in Article 2.5.3.