Kansspelautoriteit

Specifications for the remote gambling data safe (the CDB)

Version 1.1 (amendments to 1.00 highlighted)

June 5 2023

Index

Errata and changes to previous versions

Previous versions of the specifications

Previous versions of the specifications are:

- Version 1.00 authorized for public release 17 November 2020

Errata and changes

Changes to version 1.00 are marked in this version to facilitate quick identification. It remains the operator's responsibility to comply with this version of the specifications.

These changes have been marked in orange.

Preface

The revision of the Dutch Gambling Act, passed by Dutch Senate on February 20, 2019, stipulates the use of a data-based control system (Controle Data Bank, the CDB). Purpose of this system is a secure exchange of regulatory data between licensed operators and Dutch regulators.

The Netherlands Gambling Authority (Kansspelautoriteit, Ksa) describes its requirements regarding the CDB in two documents:

- The 'specifications' document contains requirements of a technical, organisational and procedural nature.
- The 'data model' document details content and processing.

Both must be used by operators when designing, operating or discontinuing the aforementioned CDB, when they apply for or already obtained a remote gambling licence under Dutch regulations.

In addition to the documents Ksa may separately provide:

- practical information like explanations, updates and schemas
- specific technical information that is likely to vary over time (like IP-addresses, encryption materials)

A review of both 'specifications' and 'data model' document is expected after approximately 12-18 months. This will be done in order to accommodate initial use phase feedback and further European level harmonisation concerning data reporting for remote gambling.

When review takes place this will be communicated through the Ksa website.

The Dutch Tax Authority has independent access to the CDB. It uses the CDB for different regulatory purposes and has the right to inspect its own (limited) data set. The Tax Authority uses its own means to access the CDB and has its own data model, access frequency and the like.

Tax Authority requirements with regard to the CDB are therefore published seprately.

The licensee has an obligation to implement the CDB in accordance with the specifications set out below.

Disclaimer

No independent permission can be derived from these requirements -or any additional information provided by Ksa regarding these requirements- for offering a particular game of chance or part thereof. Permission to offer a certain game of chance exists only and to the extent that the operator has been granted a licence for offering a game of chance as referred to in the Dutch Gambling Act.

Operators must comply with all requirements, including updates and additions. Noncompliance with these requirements is considered a violation of Dutch regulation and may lead to corrective measures by Ksa.

Under all circumstances the text of the Dutch Gaming Act -including regulations based on that Act- prevails. An operator must contact Ksa whenever there is no clarity or ambiguity about the way a certain requirement can be interpreted.

1 Introduction

1.1 About this document

The revision of the Dutch Gambling Act was passed by Dutch Senate on February 19, 2019. It establishes the national and legislative framework for gambling activities in its different forms for the purposes of ensuring the protection of public order, combating fraud, preventing addictive behaviour, protecting the rights of minors and safeguarding the rights of gambling participants.

The Dutch Gambling Act stipulates that all parties holding a remote gambling licence are obliged to implement a data-based control system for monitoring and supervising of their gambling activities by Dutch regulators: ControleDataBank (the CDB).

A total of three regulators have been entitled to use this datasafe or the CDB:
1. The regulator for the Gambling Act (Kanspelautoriteit, Ksa),
2. The regulator for Anti-Money Laundring regulation (Ksa)
3. The regulator for Gambling Taxes (Tax Office).

This document outlines the specific requirements regarding this datasafe in the context of its use by Ksa (for both regulatory tasks). The requirements apply to licenced operators, and licence applicants.

The requirements have been attuned as much as possible with requirements that are common in other areas, for example:
- European gambling jurisdictions requiring a similar datasafe system.
- audit best practises from IT or finance
- open standards set by the Dutch government
- international harmonised standards, such as ISO27001

1.2 Legal basis

Legal reference

The most important legislation around the CDB can be found in:

- articles **31h (sub 1 and 2) and 34l** of the Dutch Gambling Act (WoK),
- **article 5.3** of the Governmental Decree remote gambling (BKoa),
- and **article 4.21** of the Ministerial Regulation remote gambling (RKoa)

Lower legislation

The Ministry of Justice and Security is the legislating body and has expressed their intentions around the CDB in various other locations in the decree and regulation ('lower legislation'). See for example:

- article 4.42 section 2 BKoa (location of the CDB in The Netherlands)
- article 5.2 section 1 BKoa (access to operator equipment, including the CDB).
- article 4.11, section 2 RKoa (particular player balance data that should be in the CDB)

All these stipulations and details concerning the CDB are not explicitly repeated or summarised in this technical requirements document, although in some cases a reference may be made.

Article 4.21 RKoa

The legal reference for these Ksa requirements, Ksa data model and similar requirements from other regulators is article 4.21 RKoa. According to this article these requirements must describe at least:

a. The infrastructure and security of the CDB
b. Data storage in the CDB (see also the separate document for the data model)
c. Electronic access to the CDB
d. Procedures in case of malfunctioning of the CDB
e. Procedures regarding backup and mirrors
f. Location of the CDB and the separation of digital means regarding the gambling system

Additional requirements

Article 4.21 RKoa also provides Ksa with a legal base to further extend these requirements. Ksa has identified such requirements on several other topics, like pseudonimisation or communication and included them in this document.

Licence application, changes

The operator must provide Ksa with (full) documentation about its CDB implementation at the moment of licence application, in the case of changes and upon request from Ksa.

The operator must also participate in testing and perform assessments during these occasions.

1.3 Reading guide

Reading guide

Requirements are placed under the relevant header as much as possible, with reference to the topics listed in article 4.21 RKoa. For example, requirements regarding pseudonimisation are placed under *Data storage in the CDB*.

Specific data-related requirements to correctly populate the CDB can be found in a separate document describing the data model[1].

For easy navigation keywords are placed on the left throughout the document.

Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119[2].

The use of definitions and abbreviations is kept minimal, and described at first time use.

Ksa website

Further information around the CDB, such as detailed explanations or illustrative technical schemas may be published by Ksa from time to time, primarily on its website: www.kansspelautoriteit.nl

Versioning

Ksa may issue a new version of these requirements and the data model. Operators are obliged to use the new version when it is effectuated.

1 Kansspelautoriteit data model for the remote gambling datasafe (the CDB)

2 https://www.rfc-editor.org/rfc/rfc2119

2 The infrastructure and security of the CDB

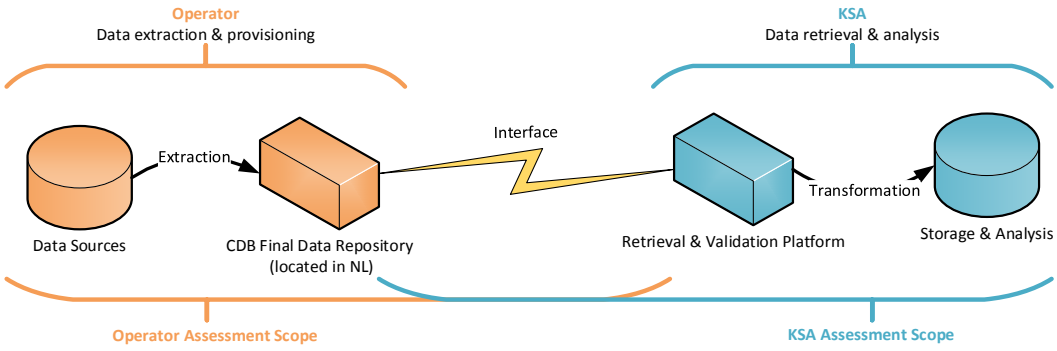
As stated in legislation, the CDB is considered a data provisioning infrastructure owned and operated by a gambling operator. This means that individual operators have a certain degree of freedom to setup their CDB infrastructure.

However, specific requirements around infrastructure and security are needed to support a safe, harmonized use of the CDB environment. Also, on the regulators end, not every single technique can be supported. For reasons such as cost-efficiency as well as that an operator's CDB environment can be used by multiple Dutch regulators.

Operators and Ksa should follow international harmonized open standards and best practises when implementing or using the CDB environment. For example the Dutch government guidelines on security that can be found here: www.informatiebeveiligingsdienst.nl (BIO version 1.0.4, guidelines in Dutch, closely related to or derived from ISO27001)

the CDB environment

The following schema illustrates the main functions of the CDB environment. The functions are derived from descriptions in legislation. For convenience an indication of expected conformity assessment scopes is included in this schema.



Segregation of data

Because of the segregation in roles and tasks of the different Dutch regulators entitled to access the CDB environment, operators must separately store the necessary data for each regulator in the CDB final data repository and provide separate access accordingly.

This is regardless of:

- the role(s) and data retrieval frequency of regulatory bodies;
- the infrastructure used by the operator;
- the required file content (segregated files could contain similar records but have a different destination).

Additionally, when an operator uses several unique customer administrations, this operator must segregate the CDB final data repository according to the number of unique client administrations.
A customer file is considered to be the complete set of customers of an operator. This customer file may comprise multiple unique customer administrations, for example for a specific game or brand. An operator needs to build a CDB for each unique client administration.

Some examples:

- a single customer administration with a single CDB environment is likely to be used by most operators. Segregation in this situation can be achieved for instance by use of different file folders or domains;
- some operators may choose to market their offering via strictly segregated brands. This could lead to the existence of multiple unique customer administrations with a single the CDB environment. In such situations the operator should apply separation of access and file location per unique customer administration;
- specific situations may even lead to the existence of multiple unique customer administrations with multiple CDB environments. For example as a result of a takeover situation, or by design (i.e. because of company security policies). Separation of access and file location per unique customer administration must also be applied, although this might be already achieved because of the use of multiple CDB environments.

Data content and format (XSD, XML), Data model.

Data intended for Ksa must be stored in the CDB final data repository according to the data model and XSD (XML Schema Definition) file structure as provided by Ksa. The operator should monitor the correct creation of data files in the CDB final data repository. E.g. validating all XML files against XSD's. The CDB final data repository must be accurate and complete, i.e. contains no more and no less data than specified in the data model.

Prior to the start of data storage and retrieval a data mapping procedure against Ksa data model must take place (see chapter 3).

Ksa will make its data model document and XSD files available separately (see Ksa website).

The operator must ensure that the correct items (such as data, files) must be extracted from the appropriate source(s). For example by use of procedures, secure connections and documentation (i.e. the data mapping outcome), including operators own gambling system, network operators and other sources.

Real Time / Near Real Time

According to article 4.12 of RKoa near real-time delivery of data must always take place. Procedures and guidance for delivery are provided in the datamodel.

Frequency of extraction and reporting triggers for information is noted in the description of the record in the "Data model for the remote gambling data safe" document. Unless otherwise specified:

- source extraction of the data must take place immediately after the original registration in that source;
- placement of the data into the CDB final data repository must take place within 30 minutes after the extraction.

Regular data retrieval

For regular data retrieval the CDB environment must support machine-based access, with automated data retrieval (i.e. by use of scripts). And it must support human-based access with manual data retrieval. Technical details required in the setup of these two variants will only be shared directly with a prospective licensee.

Ad hoc data retrieval

The CDB final data repository must contain a separate location for ad-hoc data exchange between Ksa and an operator (i.e. a file folder named 'ad hoc'). This can only be used in specific cases, for instance in an emergency recovery situation, and needs prior approval of Ksa.

Additional data (non-data model)

Additional data delivery (non-data model related) may be requested by Ksa. This could be temporary or permanent (in which case a data model change is likely to occur). This could for instance be a tailored data exchange during fraud investigation, when a request is made for exchange of personally identifiable information. Ksa and operator must agree upon the distribution method (the CDB or a different channel) and release policies prior to release of this additional data.

Additional data request

Any request for additional (non-data model related) data must contain at least:

- collected characteristics of the requested items, such as required data fields and their respective extraction frequencies;
- the reason of the request;
- exact date/time of the occasion(s) of sharing;
- data retention periods.

Normally these requests will be made in writing through the central contact of an operator, unless otherwise specified or agreed upon.

The operator must respond to the request for additional (non-data model related) data as follows:

- operators need to send a confirmation of receipt within 72 hours after the request was made;
- the operator must provide the requested information as soon as possible within a maximum window of 4 weeks.

Additional data response

Prior to placing the additional data or reports in the CDB, or any alternative channel, the operator should verify (in line with best practices for handling any data) that this data is cleared to be received by Ksa and can be stored or transferred securely.

User provisioning

To make it possible for Ksa to access the CDB using SFTP, the operator and Ksa must exchange the required connectivity information, such as device fingerprints, IP addresses, FQDN, encryption keys through a secure communication channel.
The Ksa must be able to access the CDB using SFTP without certificates.
A bilateral agreement must be made about this channel prior to sharing the connectivity information.

Security

Operators must notify Ksa immediately when breaches, data leaks, cyber attacks, errors or violations occur that (may) effect the security of CDB, or when suspicion of errors or violations occur.

Key management

Operators and Ksa must follow international best practises and their respective organisation guidelines for managing digital keys and other cryptographic means or procedures.

Algorithm selection

The algorithm selection as elaborated in the data model document must be used. This selection was made by Ksa based on current international standards and best practices, and public advice from Dutch government institutions for standardization and cyber security.
Based on, among other things, the development of technology and computing power, advice and standards may change and as a result, the current algorithm selection may prove insufficient. In that case, Ksa will publish an amended selection on its website.

Certificate usage

X.509 certificates - insofar as used in the interaction between operator and Ksa - must meet the Dutch government requirements of PKIOverheid (PKI for the government) as far as possible. The requirements for PKIOverheid are based on European standards and Dutch legislation. This allows users to trust that they are using a high-quality and reliable PKI infrastructure, which also complies with internationally accepted guidelines.

Please note that an operator is free to use other (including self-generated) X.509 certificates in company internal systems and procedures. However, this must be sufficiently reliable if used in relation to the CDB environment and evidence of this may need to be provided during internal or third party conformity assessments.

Control plan

The operator must write and manage a control plan. This plan must be formally approved, following company approval policies. The control plan – or parts thereof - must be shared with Ksa during licence application and –depending on the assessment scope- anyone performing a conformity assessment.

On a periodical basis, operators must review their control plan and adjust if necessary.

Control plan content

The control plan must contain functional specifications on (IT) systems in relation to the CDB, including:

a. access rules to determine the access that a human user or system may have to the CDB systems and/ or data (with a particular label);
b. security rules for determining from the content the protection level(s) that should be applied to a particular the CDB item (like a data field or a system);
c. categorization and/or labelling rules: rules determining the categorization and the content of category markings and/or label(s) to ensure consistent interpretation by human users and by systems.

Control plan content examples

Examples of items that should be in such a control plan:

- licence reference and validity period;
- the CDB implementation design and test methods;
- allowable data fields and formats;
- exclusions;
- recordkeeping requirements (incl. retention);
- roles and responsibilities;
- training requirements and other support requirements (Manuals, Reference like intranet pages, helpdesk, etc.);
- which individuals/organizations may have access to the CDB;
- categorization rules, labelling rules and access rules;
- location of the back-up system;
- predescibed events that trigger data extraction;
- auditing requirements, including a compliance check/reporting guidelines for the electronic systems housing the CDB data.

Controlled release

Operator must ensure a controlled release of data files to Ksa which should include mechanisms for:

- proper access control (besides user access controls, data labelling is a sound method to ensure this);
- the release. Depending on the release method desired by the operator, a submission response mechanism could be a method of choice;
- verification continuous data release. A dedicated service (e.g. a staging server) could be used to allow for a controlled release;
- secure extraction and packaging of data an automated XML generation & publication service could be used for example.

Exit plan

The operator must write and manage an exit plan. The exit plan may be a separate section of the control plan. This exit plan must be formally approved, following company approval policies.

The exit plan must be shared with Ksa during licence application and –depending on the assessment scope- anyone performing a conformity assessment. On a periodical basis, operators must review their exit plan and adjust if necessary.

The licensee must report a termination to Ksa as soon as possible. In any event, the notification must be made no later than 72 hours before the exit plan takes effect.

Internal control

The operation of the CDB described by the design, control plan or test plan should be regularly checked by an internal control official.

(third party) Conformity assessment

The operator needs to periodically perform a conformity assessment on the CDB. The initial assessment (required for licence application) will be extensive. It is expected that following assessments will consist of continuous validation.

In case of a conformity assessment:

- procedural controls must be correctly implemented and show effective data protection;
- technical controls implemented must successfully demonstrate the ability to protect information according to the requirements;
- implemented guidelines and rules (like stated in the control plan) are verified and used in accordance with requirements, such as security guidelines and audit trail methods.

This information must be made available to any party performing assessments (this could also be Ksa when performing site visits for example).

Service providers

One or more specialist service provider may be contracted to set up a CDB for the licensee. The licensee is and remains responsible for compliance with the Dutch Gambling Act and regulations based on it. Even when outsourcing to third parties, including (subsidiaries of) the parent company. The use of specialist service providers must not obstruct the supervision by the Ksa. The Ksa must not maintain supervisory relationships with third parties hired by a licensee.

3 Data storage in the CDB

Data mapping

The operator must map its source data and CDB output format in accordance with the appropriate reference format(s) (i.e. 'Ksa data model') to see if all output is delivered according to expectations. The mapping outcome or mapping result must be shared with and approved by the corresponding authority (Ksa for the Ksa data model).

For example the mapping of the CDB output data for Ksa format must be applied in accordance with the most recent version of the Ksa data model. The mapping result (i.e. a matrix) must make clear what CDB output Ksa will receive from that individual operator / client administration. Ksa must approve this mapping result.

The reference data model consists of a number of record descriptions. All descriptions must be mapped. All applicable source data - and this may include process, control or test data - must be mapped to the reference material provided. This process must include particular details such as mapping operator internal player statuses or bet types to the Ksa data model enumeration options.

Please note that deviations or impossibilities must be reported in the mapping result.

For example, transaction records are expected to apply to all operators. However the records around sports betting are not applicable for an operator offering casino games only. In this case a particular record is not applicable, however this must not be left out of the mapping process and the mapping result must contain a (brief) explanation allowing Ksa to understand this deviation from the model.

Checklist data mapping

- The most recent version of the Ksa data model, as published on the website of the Ksa, is used.
- Each element of each XML file must be present in the data mapping document.
  - For each element of the XML file the table, entity, or class must be described as well as the attribute / property as used in the system of the operator. We expect a clear mapping in, e.g. a matrix in which the mapping between the Ksa data model and the operator's data model is described.
  - The elements Record_ID, Extraction_Date, Operator_ID, Data_Safe_ID and Replaced_Record_ID are used in multiple XML files. They must be mapped for every XML file where applicable.
  - In case an element of the Ksa data model is not used (which only is possible for optional elements), this must be explicitly stated in the data mapping for each element.
  - Each value of each limitative list (enumeration) of the Ksa data model must be mapped to a corresponding value or derivation as used by the operator. In case no mapping exists, this must be explicitly stated in the data mapping.
  - For each derivation, the derivation logic must be explicitly explained in business terms. E.g. a field that is a sum of two attributes can be explained by the text Sum of all winnings minus sum of all stakes.
  - Explicitly state per element from which system it will be extracted.

Future developments	Future standardisation or best practise collection may result updated or additional reference material from Ksa. In this case Ksa must provide the necessary input and verify the updated mapping result accordingly.
Additional data fields	An operator may be required – on demand - to apply specific data fields or reporting elements, in addition to Ksa reference format.
Integrity of data	This may require an additional mapping and the results of this mapping must also be shared with and approved by Ksa. Ksa and/or an auditor should be able to verify the CDB output on integrity and be able to detect anomalies or (un)intended modification to the mapped data format.
No absent fields	In case of a mapping result against Ksa reference format (data model) where fields do not apply to a particular operator, the actual CDB output for that field must be 'null' (no empty fields, no absent fields).
Personal data	Personal data is processed in the CDB. The General Data Protection Regulation applies to this processing. The licensee is responsible for compliance with this regulation, including when hiring third parties.
Individual tailoring	It is prohibited to tailor the reference format and the mapped output to individual needs. In other words: DO NOT DEVIATE FROM THE XSDs PROVIDED BY Ksa!
Extraction	The operator extracts items (such as data, files and event logs) from the appropriate source(s) in batch, on-demand or continuous mode as defined in the mapping outcome.
Control plan	Extraction follows a controlled predefined process (e.g. with scripts) and triggered by predefined events. These processes and events must be described in the control plan.
Qualified personnel	Operator personnel are trained/qualified to make the determination whether data can be extracted and placed in the CDB. Regardless of this being done in relation to the data model or to an ad hoc on demand data request.
Logging data requests	The identity and qualifications of all operator representatives who associate a request with a piece of data will be captured and recorded for audit purposes. This record will be maintained by the operator, and will not be visible to external recipients.
Determination process	This request and data determination process is followed according to written policies and procedures (e.g. scripts), and controlled (e.g. through self-assessment or audit). A system may be available to support these procedures or scripts. If so, that system should be able to: • present all available regulations that apply to the CDB (e.g. company policies); • assist the user in determining applicable regulations, for example though a guided decision tree; • prompt the user to consider all restrictions that may apply to an information object, including proprietary information restrictions, personally identifiable information restrictions, etc.

Validation	Prior to loading items into the CDB the operator must validate the extracted items such as data, files and event logs. The operator must evaluate and improve this validation process whenever necessary. Validation must include data integrity, availability, privacy and persistence checks. The validation methods must be listed in the Control Plan. The operator has tested these methods beforehand. The entire validation process must be described in detail, monitored (with logging) 24x7 where applicable and frequently audited periodically (at least twice a year).
Documentation Sources	The operator ensures a complete description of the sources that are used. The source description must correlate to the data or report. This must be included in the operator's mapping output.
Audit Mapping	The source description must be stored and made available for licence application, testing and upon request by Ksa. An (internal/external) auditor or any other supervising entity, for example company officials like the compliance officer, a security officer, a technical lead may have access to this information. This must be included in the operator's mapping output.
Outsourcing Subcontractor	The source description may contain sources not owned and/or operated by the operator (outsourced services). In such cases the source description should contain (a reference to) an agreement between operator and the subcontractor on the purpose, availability and extraction of that source by the operator. This must be included in the operator's mapping output.
Audit / conformity assessment	In case of an audit of the sources: An identified agenda / scope (of testing, audit, etc.) must be present and correlate to the purpose of using a data source for the CDB.
Audit guidelines	Audit reports, either written manually or generated by a system that are delivered to operator and/or Ksa should be formatted according to internationally harmonized audit guidelines and should permit auditors to verify the compliance of the operator with requirements. Audit report guidelines differ by company and are usually not shared externally. Therefore a list of expectations on audit reports is placed on the Ksa website.
Release Notification	The operator will release the production level CDB and notify Ksa (and if desired other stakeholders that the operators wishes to inform). The notification to Ksa must be done in writing, must be dated, and be formally signed off by the official, responsible for the CDB. Notification must take place via email with an attachment to the email in the form of a memo/pdf including the above mentioned signature. Ksa will add these documents to the operators file. Contact details will be made available on the Ksa website.

Notification to Ksa of production level release must be done, and Ksa must acknowledge the receipt and return confirmation in writing. Notification and acknowledgement must take place prior to release of any product offering under the Dutch licence.

3.1 Pseudonimisation of data

Some data that needs to be placed in the CDB is considered Personal Identifiable Information and pseudonyms must be used instead. The appropriate data elements can be found in Ksa data model.
Please note that under specific supervision circumstances (i.e. fraud investigation) Ksa may require the operator to reveal (a limited number of) customer identities (see Chapter 2, additional data).

Operators are free to choose a pseudonym as long as:

- the pseudonym does not exceed the data field specifications (i.e. maximum characters) as required in Ksa data model;
- GDPR requirements around pseudonymisation are met (including EDPA opinions);
- the chosen prerequisites for a legally secure pseudonymisation as well as the process steps for carrying out a pseudonymisation must be documented (i.e. in the control plan) and belong to the scope of the (periodical) independent audit. Please note that a pseudonymisation may take place in several stages, for example, with the participation of one or more trust bodies;
- the pseudonymisation procedure must ensure the linkability of pseudonyms: identical pseudonyms can only be used to identify identical persons. However, the linking of pseudonymised data with identified persons without knowledge of the pseudonymisation must be avoided. Only the operator must be able to pseudonymise its customer records accordingly. Ksa should not be able to link pseudonyms (or reverse pseudonymisation);
- the operator is able to fulfil a request from Ksa to reveal (a limited number of) identities;
- the same pseudonimization process is applied in all environments in which CDB is active, such as: test, acceptance and production environment.
- appropriate security and quality measures are in place, such as:
  - good application semantics;
  - cross domain functions;
  - controlled changes;
  - anti-collusion measures;
  - security controls on the ‘data trust zone’;
  - protection against statistical analysis.

4 Access to the CDB

In the following chapter, access requirements are described from the perspective of the overall CDB infrastructure that an operator must build.

As explained in chapter 2 the CDB is considered to be a data-exchange infrastructure that can be composed of different machines, software, processes, connections, interfaces etc.

Please note that lower legislation specifies under Article 5.3 BKoa that – for the particular function of inspection or retrieval of data from the CDB- access needs to be separate for each regulator. And that both regulator and operator must not be able to modify when it resides on the final data repository.

4.1 Entities

The following parties may have access to the CDB environment via their respective interfaces.

Regulators

a. Entitled regulators that wish to inspect or retrieve data from the CDB. Each must have independent access from the other (i.e. different credentials, separate file folders). This will only be via a digital interface.
b. Ksa, as Gambling Act regulator in general, must have remote and physical access to (elements of) the CDB environment to verify the correct implementation and performance of the CDB environment. In case of investigation, licence application or change requests for example.

Operators

c. Operators must have access to the CDB environment since they are responsible for the correct implementation and must control the quality of data reporting service. It is expected that operators have both automated access (i.e. source extraction) and manual access (i.e. service management).

(independent) third parties

d. Third parties may need access in some situations. Their access is considered to always fall under the responsibility of either a regulator or an operator. For example:
   - operators may need to contract an independent auditor to perform periodical conformity assessments. This might also be imposed by Ksa as a corrective measure;
   - operators may outsource elements of the CDB infrastructure (such as maintenance or platform hosting services), and allow a service provider access to (parts of) the CDB;
   - operators may have an internal auditor / compliance officer that needs access to verify proper operation of the CDB;
   - Ksa may also outsource its work, for example Ksa can contract an independent auditor to perform work on behalf of Ksa as mentioned under b.

Access control can be implemented according to company policies of the operator, as long as access by the regulators will follow specifications (i.e. SFTP for Ksa).

Automated or manual access

All forms of access must be accommodated for as needed. Some examples:

- automated access (script on machine) and manual access (human on local computer) access by must both be accommodated;
- physically entering the machine room for maintenance or inspection;
- access to support conformity assessments (i.e. using a gateway proxy system);
- physically entering the room where the CDB is placed (Article 5: General Administrative Law Act and Article 34e WoK);
- subjecting the CDB to examination (Article 5:18 of the General Administrative Law Act);
- sealing of the CDB or the room where it is located (Article 34d WoK).

When renting computer equipment or employing service providers for your CDB, the operator must include in the contract with the lessor or service provider that Ksa can exercise the investigative powers. For example, the operator includes that a data center or the service provider will allow the Ksa to access stored data.

Identity management

Access controls must be implemented in such a way that access can be granted in a uniform, stable manner so tasks like data transfers can be performed smoothly and without interruptions.

Any form of access to the CDB must be restricted to authorized individuals, men or machines from both the operator and the regulators.

Separation of duties

With proper identity and access management (i.e. credentialing, privilege management) to service all entities that require access. If particular credentials are required (by anyone entitled for access) those credentials must meet the operator's company security standards.

The operator must also:

- put access management in place according to open standards where possible;
- enforce separation of duties for all Operator employees and employees of subcontractors involved in the CDB, both in technical management or procedural management;
- include control measures on services and not just on humans or machines. In particular services around handling data, ensuring that data files are only transferred if *fit for purpose* (i.e. validated against the XSD, correctly stored according to filing requirements, properly marked if that is required by operators security requirements).

Logging & monitoring

All access to the CDB and actions that were taken must be logged in the appropriate (audit) log. Access logging, data submission response, or data download should be part of the logging and monitoring services.
Logging and monitoring should take place in such way that it can support a sound governance and any conformity assessment of the CDB.

Documentation

The procedures for access must be documented (i.e. in the control plan) and shared with Ksa when applying for a licence and upon request.

5 Procedures in case of maintenance or malfunctioning of the CDB

Scheduled maintenance

An operator may, with at least five days prior notice, decommission its CDB environment or parts thereof for scheduled maintenance purposes. Further information about notifying Ksa regarding maintenance on CDB is available on Ksa website[3].

An operator must perform scheduled maintenance outside of the peak hours of its company, whilst ensuring that:

- all required data is still extracted from source systems according to the data model and stored securely. For example by temporary storage on a secure intermediate server;
- maintenance outcome is formally approved following company policies before the CDB is turned back on;
- the data must be included in the CDB storage platform for retrieval by regulators immediately after.

Please note that temporary storage solutions are considered to be part of the overall the CDB infrastructure and therefore all requirements from regulations and Ksa specifications are applicable.

Malfunctioning

An operator should monitor the operation of the CDB and compliance with the data model on data placed in the CDB. Malfunctions or shortcomings must be reported to Ksa as soon as possible but at least within 72 hours.

Emergencies

In case of emergencies, the operator may decommission the CDB or parts thereof for repairing purposes without prior notice. In these cases the operator must inform Ksa as soon as possible, no longer than 72 hours after decommissioning the system.

Accountability must be given afterwards in writing within a tome window of 4 weeks.

Data that was generated in the gaming system during the period in which the CDB environment was unavailable must be filed (i.e. using a backup system) and restored in the main the CDB repository as soon as possible after recovery. This must be logged and logs must be made available for assessment purposes.

The operator must provide information in its control plan how this is achieved securely to prevent breaches like data loss or manipulation of data.

[3] At the moment of writing: https://kansspelautoriteit.nl/voor-zakelijke-aanbieders/meldplicht/

Communication around problems

Maintenance announcements or emergency notifications must be done by the regular communication channels unless otherwise specified (i.e. Ksa may open a specific channel for emergency notifications in case regular channels seem inconvenient).

Ksa may experience technical or functional problems. Or issues with content in the CDB repository. In this case Ksa will contact the operator concerned through the regular channels to find a solution.

In some cases multiple operators or multiple regulators may experience similar technical problems. In such case Ksa will coordinate this, ensuring a central point of contact.

6 Procedures regarding backup, mirrors and retention

The operator is responsible for the correct implementation of the CDB environment, including its availability and data loss prevention. See also Chapter 2 of this document or legislation around the CDB.

Different solutions are available and operators may choose solutions that fit its business operations best.

Backup

All operators are obliged to keep a backup system that will ensure availability of the data while allowing recovery in case of file/folder deletion or corruption. Ksa needs to be informed about the location, specifications and operation of the backup system and changes thereof. The operator must specify this in its control plan.

Mirror

If a mirror repository or similar solution is available, it should be on a secondary location physically separated from the original the CDB final data repository and separated from the gaming systems. This mirror will allow the CDB to keep working in the event of hardware failure, reducing lost availability. Such a mirror may not also serve as the back-up solution

Retention

Minimum retention period of the data in the CDB final data repository is 12 months counting from the moment of the compulsory registration.
Operators must guarantee this retention in their control plan and also in their exit plan.

7 Location of the CDB and the separation of digital means regarding the gambling system

The complete CDB environment may be composed of several systems, services etc. according to the operators choice of implementation.

Besides any requirements from legislation or Ksa specification, these different components:

- may be dispersed over different virtual and physical locations, within the EER;
- must be easily accessible for Ksa (e.g. trough one uniform interface portal);
- must meet the operator's company security standards.

The operator must describe its complete CDB environment in a written statement in either Dutch or English, including a schema of the configuration at the moment of licence application and/or upon request by Ksa. This written statement shows that all requirements have been met and that the design matches with all that the operator (intends to) offer under the Dutch gambling licence. The operator is free to send any additional information, such as for example a video, explaining how the CDB environment is designed and operated.

Separated server

Location

The legislation requires that the CDB final data repository must be located in the Netherlands physically separated from the operators gambling system. Both may be located in the same data centre if an operator chooses to do so, however data stored in this main the CDB final data repository must be logistically and safely separated from any other data.

Intermediate or staging server

If an intermediate or staging server is used by an operator in its the CDB-environment than this component must be secured (e.g. limited access) and physically separated from the operators gambling system. For instance data source extraction ('data capture') may be run on such a staging server. Similary an intermediate server might be used in case of emergencies.

8 Testing

This chapter is about test procedures between operator and Ksa, for example during licence application or when changes to the CDB environment are made.

This testing deals primarily with the technical interface and (automated) data exchange between Ksa and operator ('the CDB front-end'). On a case by case basis such testing could also have other objects in scope, i.e. new communication techniques. The aim of Ksa for testing is to technically and functionaly assess the working of the operator's CDB and its readiness to be connected to the production environment of Ksa.

Please note that this testing differentiates from the conformity assessment by an independent third party, as mandated by the legislator. That assessment deals with the correct implementation of the CDB environment by the operator ('the CDB back-end').

Production test

Prior to any production level use of the CDB environment testing with Ksa must be done. Testing will take place based on a test plan that has been approved by Ksa. Once the testing has been completed and Ksa has approved the subsequent test results further use of the CDB is allowed.

Test plan

For each case a specific test plan must be agreed upon between each operator and Ksa. This is because the CDB environments are likely to vary among operators. And availability of testing personnel and equipment needs to be organized. Test participants should perform tests and capture results as stated in this test plan.

Ksa cannot approve further use of the CDB environment if a test plan cannot be agreed upon, individual tests are not executed or fail and when testing is not possible. More information about the completion or discontinuation of the test program is included in the Ksa Policy Rules for Licence Applications.

Test requirements for licence application

For licence application Ksa must provide minimum, appropriate test requirements (i.e. on its website). Ksa shall also provide appropriate test environment(s).

Among others, the following examples could be part of a test programme during application:

- connection tests (volume, bandwidth, latency, availability, protocol, etc.);
- encryption tests (key exchange, decryption, decompression, etc.);
- data transport tests;
- data quality tests.

In other cases, like change or decommissioning of the CDB environment, test requirements, personnel and equipment needs to be tailored to the situation.

Operators must take into account the time that is necessary for performing data mapping and testing procedures. They must therefore notify Ksa in advance in order to agree upon a test plan in time (see also chapter 9). The change can only be effectuated after testing has been completed and approved.

Other test occasions

Besides the formally required pre-production tests, Ksa and operators may enter into other testing. For example:

- Ksa is legally entitled to perform site visits. Depending on the occasion this may also include testing. Operators must grant access and assist with testing accordingly;
- on a voluntary basis Ksa and an operators may decide to perform tests for other reasons. Like preliminary testing in preparation for licence application. Or development-level testing. Please note that voluntary also means that participation is on a request-basis and requests may not be granted. No rights can be derived from the results of these types of testing.

Test Outcome

Ksa informs the operators about the outcome of tests, as agreed upon in the approved test plan.

9 Changes

Ksa must be informed in advance by an operator when its CDB operations change, including circumstances regarding the operator's business. A detailed explanation (including examples of the alterations) must be submitted along with the notification.

For some specific types of changes a submission window is stated. Incorrect application may result in corrective measures from Ksa. On the other hand such a timeframe cannot always be provided by Ksa as this depends on the nature of the change:

- some changes may require full investigation and may even impact licence conditions. This can be the case when for example a casino game operator decides to add betting to its product range;
- other changes may be handled within 5 working days. An example of this type of change is maintenance (see chapter 5);
- some changes have a recurring character (weekly operating system updates) and can be handled via a single notification in advance (instead of a weekly change notification, 72 hours afterwards). Such notification must be repeated every 6 months.

A guidance on notifying changes is available on Ksa website. Notification on changes regarding CDB must include:

- Type of change: e.g. scheduled maintenance, general change, specific change or data leak
- Description and impact on CDB of the change
- Date and time when change takes place
- Duration to complete the change

General changes

Changes that do not affect the way in which the CDB environment is used can commence without prior notification to Ksa. In these cases Ksa must be informed within 72 hours after commencement. Some possible changes in this category are:

- Regular software updates
- Change in processes
- Revision of documentation
- Some types of security updates and emergency fixes (i.e. workarounds or patches)

Specific changes

Other changes are likely to have high impact on the CDB environment and may require additional preparation by the operator or even approval by Ksa. In case of a substantial change, which would affect operations to an extent where the CDB can possibly not be used, this must be notified to Ksa at least 3 months in advance and the change is not allowed to commence without prior approval from Ksa.

10 Communication

Contact between operator and Ksa

Ksa provides a central point of contact for operators to send questions, change notifications, requests etc.
Questions about the tax part of the CDB or about tax audit files can be asked at the tax office[4]. Other questions about CDB can be directed to Ksa.
Questions while in preparation of your application should be sent to the general contact address of the Ksa[5].
When already working on an application in the digital portal or already submitted an application one must use the contact form for applicants for a Koa license. Requests intended for the tax authority will be forwarded by Ksa. The tax authority will handle these requests.

The operator must also provide a central point of contact for Ksa.

All communication is in the Dutch language. An English-language courtesy translation can be added, for example to shorten response times. License holders and providers who have applied for a permit must be available during Dutch office hours (Monday through Friday from 9:00 a.m. to 5:30 p.m.), Dutch national holidays excluded. These days can be found in the General Extension of Time Limits Act. Non-Dutch public holidays or other time zones, are no reason for exceeding response time limit.

Communication with third parties

Communications around the CDB must take place between Ksa and an operator representative, not between Ksa and any third party acting on behalf of this operator.

In some cases a meeting with both Ksa, the operator and a representative of a third party may be possible. This could for example be necessary during the test phase when technical aspects that have been outsourced need to be discussed.

XSD / XML, File structure, Update

The Ksa internet website is the central information platform regarding requirements, specifications, procedures and other information regarding the CDB (like changes). Operators should regularly check this website.

[4] At the moment of writing: www.odb.belastingdienst.nl or koa@belastingdienst.nl.

[5] At the moment of writing: https://kansspelautoriteit.nl/contact/ or info@kansspelautoriteit.nl.

Afzendgegevens

Kansspelautoriteit
Anna van Buerenplein 45A
2595 DA Den Haag
Postbus 298
2501 CG Den Haag
www.kansspelautoriteit.nl