

30.03.2020 | Topic [Authorisation requirements](#)

Guidelines on applications for authorisation for crypto custody business

Content

- 1. Basic guidance for applications for authorisation
- 2. Guidance on the process on the basis of the transitional provision under section 64y of the KWG
- 3. Guidance on the contents of applications for authorisation
 - a) IT requirements
 - b) Reliable and qualified managing directors
 - c) Number of necessary managing directors
 - d) Prevention of money laundering and terrorist financing
 - e) Fee for the grant of authorisation

These guidelines provide undertakings intending to submit an application for authorisation for crypto custody business within the meaning of section 1 (1a) sentence 2 no. 6 of the KWG with initial guidelines on the aspects, which BaFin considers to be particularly important for the authorisation process.

(This English translation of the original document is non-binding and for convenience purposes only.)

The German Act Implementing the Amending Directive on the Fourth EU Anti-Money Laundering Directive (Federal Law Gazette I of 19 December 2019, p. 2602 (Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie) has included crypto custody business in the German Banking Act (Kreditwesengesetz – KWG) as a new financial service. Since the Act came into force on 1 January 2020, undertakings wishing to provide this service are required to apply for an authorisation from BaFin.

This guidance provides undertakings intending to submit an application for authorisation for crypto custody business within the meaning of section 1 (1a) sentence 2 no. 6 of the KWG with initial guidance on the aspects which BaFin considers to be particularly important for the authorisation process. For guidance concerning the definition of crypto custody business, please refer to [BaFin's guidance notice](#) on this subject.

The formulated expectation expressly applies for crypto custody business, but not for existing administrative practice in relation to banking business or other financial services. This guidance do not constitute an exhaustive list. The relevant statutory provisions apply, and the applicable circulars, guidance notes and summaries provided by BaFin and Deutsche Bundesbank should be taken into consideration.

Undertakings may address any crypto custody business-related questions directly to [BaFin's Group IT supervision](#) (kryptoverwahrung@bafin.de) or to [their Deutsche Bundesbank regional office](#). Any information transmitted digitally should always be provided by means of secure [communication channels](#). BaFin's Directorate IF is responsible for any questions as to whether an activity requires authorisation.

1. Basic guidance for applications for authorisation

The authorisation process for undertakings wishing to provide crypto custody business within the meaning of section 1 (1a) sentence 2 no. 6 of the KWG is based on section 32 (1) of the KWG and is thus comparable with established authorisation processes for banking business or other financial services which were already regulated before the new regulation came into

force. The relevant regulations therefore also apply, in particular the German Reports Regulation (Anzeigenverordnung, [AnzV](#)). Section 14 of the [AnzV](#) stipulates the reports which must be provided and the documents which must be submitted. Applicants can therefore consult the [notice from Deutsche Bundesbank on the granting of authorisation to provide financial services of 6 July 2018](#) for further information.

Provided that the specific business model is not limited to providing custody, management and backup services for cryptoassets within the meaning of section 1 (11) [no. 10](#) of the [KWG](#), but rather to financial instruments under Annex 1 Part C of Directive 2014/65/EU ("MiFID II"), an authorisation requirement for other banking business or financial instruments within the meaning of the [KWG](#) may also apply. In those cases where business activities also cover financial instruments within the meaning of [MiFID II](#), the authorisation process might be based on Delegated Regulation (EU) 2017/194 instead of section 32 (1) sentence 1 of the [KWG](#). Further information on authorisation as an investment firm within the meaning of [MiFID II](#), which will be required in such cases, may be found on [BaFin's website](#).

Complete application documents must be submitted in order for authorisation to be granted. Applicants should not therefore submit any incomplete applications for authorisation. This also applies in relation to the transitional provision stipulated in section 64y of the [KWG](#) and to the granted time limit of 30 November 2020 (see [no. 2](#) for further information). If certain information and documentation is not yet available, a brief justification should be provided, with an indication as to when the applicant expects to be able to submit this. In the event that questions of supervisory law already arise during the preparation of the full application for authorisation and the answers to these questions are considered likely to be critical for the granting of this authorisation, undertakings may contact [BaFin](#) directly or else their Deutsche Bundesbank regional office. Undertakings which do not fall under the scope of the transitional provision may only begin to operate once [BaFin](#) has granted them a legally effective authorisation.

Please note that the application must be signed by persons authorised to represent the undertaking. As an alternative, the application may be submitted digitally, exclusively in accordance with the requirements of section 3a of the German Administrative Procedure Act (Verwaltungsverfahrensgesetz – [VwVfG](#)), [i.e.](#) as a rule by means of documents signed with a qualified electronic signature. Information on the legally valid transmission of electronic documents may be found on [BaFin's website](#).

In addition, documents and declarations may be submitted in a simple digital format if the relevant statutory provisions do not require submission of the original or a handwritten signature. This will apply, for instance, in case of the submission of curricula vitae (section 5a (1) sentence 2 of the [AnzV](#)) and statements of assurance (section 5b (2) sentence 2 of the [AnzV](#)) which require handwritten signatures. Documents submitted digitally should always be sent by means of secure communication channels, [e.g.](#) PGP or S/MIME-encrypted e-mails. Further information on the available methods may be found on [BaFin's website](#).

2. Guidance on the process on the basis of the transitional provision under section 64y of the [KWG](#)

Through the transitional provision in section 64y of the [KWG](#), the legislature provided undertakings which were already operating before the [GwRLÄndG](#) entered into force with sufficient time to adjust their internal systems and processes in line with the supervisory requirements laid down in the [KWG](#). However, the transitional provision grants notional permission as of 1 January 2020, so that undertakings are thus already institutions within the meaning of the [KWG](#). [BaFin](#) therefore expects that undertakings will already have made appropriate efforts to rapidly comply with the statutory requirements since 1 January 2020. Applicants which have not adjusted their processes in line with the supervisory requirements within the transitional period stipulated by legislature, despite their submitting an application, will not as a rule have provided any evidence as to the orderly conduct of their business. The requested authorisation would be denied in such cases. [BaFin](#) therefore reserves the right to make inquiries so as to obtain further information on the preparatory activities implemented and planned, even before authorisation is granted. Insofar as undertakings have not yet fulfilled certain requirements upon submission of their application for authorisation, these undertakings should be able to explain the reasons for this and to be able to present a timetable for rapid implementation. Undertakings should independently analyse the (technical) risks which they envisage during the current implementation process and how they intend to deal with these.

Erlaubnisverfahren Kryptoverwahrgeschäft



(c) BaFin

BaFin expressly points out that the transitional provision does not refer to services requiring authorisation which were already subject to this authorisation requirement before this legislative change entered into force. Reference is made to the published [guidance on the interpretation of section 64y of the KWG](#).

3. Guidance on the contents of applications for authorisation

An application for authorisation to conduct crypto custody business within the meaning of section 1 (1a) sentence 2 no. 6 of the KWG must document, inter alia, sufficient initial capital of at least EUR 125,000 and that the undertaking has reliable owners as well as reliable and qualified managing directors. A business plan must also be attached to the application. As well as planning encompassing the balance sheets and profit and loss accounts for the first three full financial years, in particular this must cover the undertaking's organisational structure and present its intended internal control mechanisms. Accounting must be in accordance with the [German Regulation on the Accounting of Banks and Financial Services Institutions \(Kreditinstituts-Rechnungslegungsverordnung – RechKredV\)](#). Undertakings must ensure that they have a proper business organisation. Due to the technical focus of their business activity, in particular information must be provided regarding their IT strategy and IT security (cf. no. 3 (a) below). The specific information and documentation which must be submitted is stipulated in section 32 of the KWG as well as the specific requirements of the AnzV. Section 14 of the AnzV in particular must be complied with for the authorisation process.

The requirements of the German Holder Control Regulation (Inhaberkontrollverordnung – InhKontrollV) also apply for crypto custody business applications for authorisation in regard to the documents which must be submitted for natural persons and legal entities with a significant role in the undertaking. [The guidance notice on holder control of 27 November 2015](#) may therefore serve by way of guidance. The ["list of enclosures" in no. 6.4 of the "acquisition-increase" form in the Annex to the InhKontrollV](#) provides an overview of the enclosures which must be submitted, although different submission and documentation obligations apply (cf. section 14 (5) of the AnzV).

In addition, the supervisory authority's expectation regarding the conduct of crypto custody business is outlined below in terms of selected aspects:

a) IT requirements

Adequate IT security is an integral part of a proper business organisation within the meaning of section 25a of the KWVG and must be outlined along with the institution's intended internal control mechanisms (section 14 (7) no. 3 of the AnzV). Both the Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement – MaRisk) and the Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT – BAIT) must be applied to the concrete business activity – while always bearing in mind the principle of proportionality – and must be taken into consideration in the risk management system.

In particular, BaFin expects information concerning the specific characteristics of the IT systems as well as the IT processes implemented. This information must be submitted by undertakings benefiting from the transitional provision laid down in section 64y of the KWVG as well as undertakings which submit an application for authorisation for crypto custody business within the meaning of section 1 (1a) sentence 2 no. 6 of the KWVG irrespective of this transitional provision. In the information provided in the application for authorisation, the explanation of the measures implemented should focus on the security of the cryptographic keys. The documents to be submitted comprise, in particular, a presentation of the security strategy, handling of security incidents and a risk assessment for the undertaking as well as a presentation of existing technical and organisational methods for the use of cryptographic keys.

On the basis of its described business model, the undertaking should outline how the cryptoassets are held in custody from a technical point of view, i.e. which form of storage is used (e.g. "hot wallet", "cold wallet"), and whether and how cryptoassets are held in custody for individual customers in separate or pooled wallets.

A comprehensive description of the IT systems implemented should be provided on the basis of the description of business activity. The information and documents to be submitted should cover the following points in particular:

- The undertaking should submit a detailed presentation of its **business strategy** in relation to the planned activity.
- A detailed presentation of its **IT strategy** must be provided which complies with the requirements laid down in section AT 4.2 of MaRisk. In particular, this involves the management board defining a long-term IT strategy which presents its objectives as well as the measures to achieve these objectives.
- A comprehensive description of the **architecture of the IT systems** should be attached. This should include network and backup elements as well as specific hardware for custody of the cryptoassets.
- A **presentation of the security strategy** must also be attached to the application. The technical and organisational precautionary measures implemented must be outlined as well as the encryption methods used.
- **Details should be provided of any (significant) outsourcing and of any cloud solutions used.** Any partners involved in the conduct of crypto custody business should be indicated and their respective roles outlined. Section AT 9 of MaRisk and the guidance notice "Guidance on outsourcing to cloud providers" should also be taken into consideration.
- The undertaking should perform a **risk assessment** and outline effects and measures, e.g. in relation to the **protection objectives**, the **loss of cryptographic keys** as well as other key data and the IT infrastructure.
- In addition, a detailed description of the **crypto concept** must be submitted, incl. an IT description of the cryptographic functions and methods used. Details must be provided of the existing **contingency plan** as well as the measures implemented to avoid the loss of the cryptoassets held in custody.
- The undertaking should identify the roles with access to sensitive data and the cryptographic keys held in custody and provide details of its **role-based security concept** or its **user access management** (cf. no. 5 of BAIT).
- The applicant should submit a **description of the monitoring procedures set up**, such as the system monitoring process which it has implemented.
- This information must be provided in line with the principle of proportionality, and always in relation to the concrete business model. This information should focus on the undertaking's specific situation.

b) Reliable and qualified managing directors

The managing directors of an institution must be qualified and reliable and devote sufficient time to the performance of their duties (section 25c (1) of the KWVG). This also applies for the conduct of crypto custody business within the meaning of section 1 (1a) sentence 2 no. 6 of the KWVG. A managing director's lack of qualifications will constitute a ground for denial of authorisation (section 33 (1) no. 4 of the KWVG).

In principle, on the subject of the reliability and qualifications of managing directors applicants may consult the "[Guidance notice concerning managing directors pursuant to the KWVG, the Payment Services Supervision Act \(Zahlungsdienstenaufsichtsgesetz – ZAG\) and the German Investment Code \(Kapitalanlagegesetzbuch – KAGB\)](#)" which likewise applies for crypto custody business. The documents required for the review of whether the applicable requirements are fulfilled must include, in particular, a curriculum vitae with the applicant's handwritten signature as well as a certificate of good conduct for presentation to an authority (section 30 (5) of the German Federal Central Register Act (Bundeszentralregistergesetz – BZRG)) as well as an excerpt from the Central Trade and Industry Register (section 150 of the German Industrial Code (Gewerbeordnung – GewO)). BaFin has published a [check list as an annex to the above-mentioned guidance notice](#) which specifies the documents which are to be submitted.

A managing director will be qualified to manage an institution within the meaning of the KWVG if this person has sufficient theoretical and practical expertise in the relevant areas of business as well as management experience (section 25c (1) sentence 2 of the KWVG). In case of crypto custody business, in conducting its review BaFin will take into consideration both the size and the structure of the undertaking as well as the fact that crypto custody business is a new financial service which was unregulated until 1 January 2020. BaFin has already adjusted its decision-making criteria in relation to the managing board's IT expertise for traditional banking business (cf. [BaFin-Journal 12/2017, p. 15](#)). Since crypto custody business is essentially based upon technical processes and the security of the cryptographic keys held in custody is particularly important, BaFin will follow these decision-making criteria in relation to crypto custody business. In case of crypto custody business, it allocates a particular status to the technical expertise of a managing director and will therefore – in relation to this field alone – comprehensively assess this person's technical expertise, e.g. a relevant course of study and extensive practical experience of IT security issues, in terms of the managing director's qualifications "in the relevant areas of business" (section 25c (1) sentence 2 of the KWVG).

BaFin will assess as practical expertise in the field of crypto custody business activities which are of concrete relevance – i.e. which have an appropriately elevated hierarchical status – for an undertaking which falls under the scope of the transitional provision in section 64y of the KWVG. However, it is expected that managing directors will also use the period of time granted by the transitional provision in order to develop areas of expertise which they have not yet completely mastered.

In addition, in justified individual cases BaFin will review to what extent the human resources and organisational structure of the undertaking is suitable overall in order to temporarily compensate for a lesser degree of expertise on the part of a specific managing director who serves on this undertaking's management board. These are always decisions which are made on a case-by-case basis, while also taking into consideration the size and the structure of the undertaking as well as the areas of business which are concretely conducted.

c) Number of necessary managing directors

Insofar as an institution exclusively holds cryptoassets in custody within the meaning of section 1 (11) no. 10 of the KWVG, in principle – by way of a reversal of section 33 (1) no. 5 of the KWVG – the appointment of only one managing director will suffice. However, a different situation may apply if the relevant cryptoassets are (also) included in another category of financial instruments in section 1 (11) of the KWVG or if the institution conducts other types of business.

Nonetheless, BaFin expressly points out that, irrespective of this provision, the appointment of one or more further managing directors may be necessary from a supervisory point of view in specific individual cases. The implementation of the dual control principle on the undertaking's management board will certainly be necessary if, on the basis of the size of the institution and the scope of its business activities, a proper business organisation within the meaning of section 25a of the KWG cannot be ensured with only one managing director. BaFin will review this on a case-by-case decision on the basis of the documents submitted for the authorisation process. For this reason, too, an organisational chart must be attached for the authorisation process which indicates the responsibilities of the management board (section 14 (7) sentence 1 no. 2 of the AnzV). The documents submitted should also indicate that the institution has sufficient human resources and a sufficient technical and organisational structure in order to comply with the statutory requirements (section 25c (4) and (4a) no. 4 of the KWG). In addition, BaFin points out that, under section 25c (1) of the KWG, managing directors are required to devote sufficient time to their activity.

d) Prevention of money laundering and terrorist financing

BaFin expressly points out that the obligations under the German Money Laundering Act (Geldwäschegesetz – GwG) must already be fulfilled by the new obliged entities in case of temporarily valid authorisation on the basis of the transitional provision in section 64y of the KWG. Accordingly, prompt fulfilment of these obligations is expected, irrespective of the progress of the authorisation process within the scope of the transitional provisions in section 64y of the KWG. However, BaFin will apply the principle of proportionality in relation to possible sanctions in a specific case, if particular requirements mean that a certain period of time is required for operational fulfilment. Moreover, in the event that institutions intend to outsource internal precautionary measures in the area of money laundering prevention, reference is made to the obligation of prior notification under sections 6 (7) of the GwG and 25h (4) of the KWG. In addition, BaFin must be notified of the appointment of the money laundering officer and the deputy money laundering officer pursuant to section 7 (4) of the GwG. A [form](#) for this purpose is available on BaFin's website.

e) Fee for the grant of authorisation

The fee for the grant of authorisation is as stipulated in the Annex to the German Regulation on the Imposition of Fees and Allocation of Costs pursuant to the FinDAG (Verordnung über die Erhebung von Gebühren und die Umlegung von Kosten nach dem Finanzdienstleistungsaufsichtsgesetz – FinDAGKostV). In the event that only an application has been submitted for crypto custody business within the meaning of section 1 (1a) sentence 2 no. 6 of the KWG and cryptoassets within the meaning of section 1 (11) no. 10 of the KWG are held in custody, managed or protected for third parties, a fee of EUR 10,750 will apply. This fee will be due upon grant of authorisation. Please note that a fee will apply if authorisation is denied and also in case of the withdrawal of an application for authorisation (section 3 (2) of the FinDAGKostV).