Explanatory notes

to the form for registration
as a crypto service provider

DeNederlandscheBank

EUROSYSTEEM

Explanatory notes to the request for registration form for registration as a crypto service provider

If you provide crypto services and are subject to the registration requirement (see Section 2.4 of this document), you can use the request for registration form to apply for registration. We register each crypto service provider to assess their risks of money laundering and terrorist financing and form an opinion on their ability to manage these risks as required by the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financiering van terrorisme – Wwft*) and the Sanctions Act (*Sanctiewet 1977 – Sw*).

We will do everything in our power to ensure a smooth and straightforward registration process. You can contribute to the process by supplying complete and accurate information. These explanatory notes list the information we need from you to handle your request for registration.

Contents

1 General

1.1 Company data

We would like you to provide us with a number of details about your company. We also ask that you submit a number of documents, including a certified copy of the notarial deed containing the company's articles of association. If you do not yet have a copy of the notarial deed containing the company's articles of association, a final draft version will suffice for the purpose of handling your request for registration. Please note that we will not decide on your request for registration until we have received a certified copy of your company's articles of association.

Please make sure that the object described in the articles of association actually reflects the services that your company will provide.

You must also provide an extract from the trade register in the country of your incorporation. In the Netherlands, this is an extract from the Chamber of Commerce.

1.2 Contact details of external consultant

We recommend that you engage the services of a consultant to assist you in the request for registration process. Practice has shown that requests are often more complete and of a substantially higher quality if applicants seek expert advice, for example from a legal expert who specialises in the *Wwft*. This enables us to handle well-substantiated requests for registration more quickly and more efficiently. Please note that the management board must always be aware of the contents of the request for registration and be able to substantiate it, even if you decide to use the services of an external consultant.

If you decide to use the services of an external consultant, please also provide us with their particulars.

1.3 Criteria for registration

Your company is a crypto service provider if it provides, in a professional capacity or on a commercial basis, services for the exchange between virtual and regular currencies, or services for the provision of custodian wallets, or both. Examples include a website on which individuals or companies can buy or sell cryptos in exchange for fiat currencies (e.g. euros or dollars) and a website on which they can have their cryptos stored digitally.

Section 23b of the *Wwft* obliges crypto service providers to register. In order to determine whether your company qualifies as a crypto service provider, the following questions must be answered:

1. Do your company's activities meet the definition given in the law?
   If so, you must apply for registration. If you are in doubt about the legal qualification of your activities, we recommend that you consult a legal expert.
2. Does your company provide the services in a professional capacity or on a commercial basis?
   If so, you must apply for registration. Our Open Book on Supervision web pages explain this criterion in further detail: https://www.toezicht.dnb.nl/en/2/50-237989.jsp
3. Is your company looking to provide the services in or from the Netherlands?
   If so, you must apply for registration. Our Open Book on Supervision web pages explain this criterion in further detail: https://www.toezicht.dnb.nl/en/2/50-237987.jsp

2 Business plan

Together with the request for registration form, you must submit a business plan. We use this to gain an understanding of your company.

We expect you to include at least the following elements in this plan:

- A **diagram illustrating the activitie**s your company will perform, including the transaction flows
- The company strategy, including
  - The targeted market share
  - The envisaged origin of your customers
  - A well-considered description of the company's growth ambitions, including expected revenues from crypto services
  - A SWOT analysis. This is an analysis of your company's strengths and weaknesses, opportunities and threats, presenting, in matrix form, the potential success of your proposed activities. Based on a SWOT analysis, you can define objectives and subsequently devise a strategy for achieving these objectives.
  - The company's partners or chain partners

3 Policymakers (including holders of a qualifying holding)

If you submit a request for registration as a crypto service provider, you must also submit for each policymaker (management board member, supervisory board member, co-policymaker, shareholders ≥10%) with the form 'Initial assessment crypto service provider'. Remember that collecting the necessary documents that must be enclosed with the form may take some time. For example, in some situations you may need to obtain a criminal records extract.

You can only be registered as a crypto service provider if you meet all statutory requirements - which include a positive assessment decision for all policymakers.

4 Governance

4.1 Organisational structure

Please submit an organisation chart that clearly shows your company's organisational structure and lists individuals related to the company, such as shareholders.

4.2 Transparent control structure

We also ask that you provide a description of the company's control structure. This is because the law requires that we are able to determine whether your company has a transparent control structure. In short, this means that its formal control structure must be the same as the actual one. The control structure must not obstruct adequate supervision. The aim of this statutory provision is to ensure that the organisational structure in which the activities of the control structure are performed does not deviate from the legal structure in which the activities are embedded. A deviating organisational structure impedes adequate supervision of your company, as it could prevent us from detecting risks to which your company is exposed.

As part of a transparent control structure, you must be able to specify the policymakers within your organisation. Accordingly, your company's management board must consist of one or more natural persons (i.e. not legal entities). The management board must be registered as such in your company's Chamber of Commerce records.

Group relationships

If your company is part of a national or international group or a group of affiliated companies operating within or outside the EU, we would like to see a description of the group's decision-making tree and the role that your company plays in this.

Director-major shareholder (DMS) structure

Does your organisation have a control structure involving a natural person who is both a major shareholder (even if indirectly) and an executive director, or a comparable control structure? A structure of this kind warrants special attention to balanced corporate governance. Governance is defined as the division of duties, responsibilities and authorities. This division must be aimed at balancing the influence of those directly involved in the company and its operations, particularly its executive directors, non-executive directors and shareholders. It is important that the company at all times has expert and balanced operational management with adequate checks and balances and appropriate incentives. For example, your company's compliance officer or department must be able to exercise sufficient countervailing power against the unit or department that is responsible for the company's commercial decisions. In the absence of adequate countervailing power, a DMS may exercise an unduly large influence on the company's day-to-day management. This could adversely affect compliance with the *Wwft* and the *Sw*.

If your company has one or more DMSs, you must provide evidence in your request for registration that you have sufficiently mitigated the vulnerabilities attached to a control structure of this kind. This may include putting adequate arrangements in place to ensure that carefully considered decisions are taken in the event of conflicting interests between the company and the DMS.

5 Sound operational management

Section 23j of the *Wwft* provides that you must set up your company's operational management in a way that guarantees sound business operations. This means that you must analyse the operational risks to which your company is exposed and take measures to mitigate those risks. We always assess your company's sound operational management proportionately. This means that we base ourselves on the risks relevant to your organisation when assessing whether you comply adequately with the requirements pertaining to operational management.

Our assessment focuses on several aspects, which include the following:

- general principles of operational management under the *Wwft* and the *Sw*
- compliance and audit under the *Wwft* and the *Sw*
- reporting procedure under the *Wwft*
- outsourcing under the *Wwft* and the *Sw*
- training and eduction under the *Wwft* and the *Sw*

Below, we describe these aspects in further detail. The basic idea is that you must demonstrate that your company can comply with the relevant provisions of the *Wwft* and the *Sw* for each aspect by means of its sound operational management.

5.1 General principles of operational management

As a minimum, your company must base its operating procedures on the following six principles:

- A clear, balanced and adequate organisational structure.
- A clear, balanced and adequate distribution of duties, authorities and responsibilities (governance).
- Adequate recording of rights and obligations.
- Unambiguous reporting lines.
- An adequate information supply and communication system.
- Transparent documentation of the company's operational management, which is reviewed at regular intervals.

Hence, your company must have a clear, balanced, and adequate distribution of duties and authorities in place at all levels and in all units of the company. Reporting lines must be in tune with the organisational structure.

The division of tasks and the reporting lines must be documented and communicated throughout the company to ensure that all levels of the company have full knowledge of their duties, authorities and responsibilities, their role in the organisation and the control process, and how they are held accountable. If you find any shortcomings or deficiencies, you must ensure that the organisational structure and the procedures and measures are changed to ensure that these are remedied.

Your company must also ensure that policies, procedures and measures are implemented and systematically tested. You must clearly document how this is done.

5.2 Compliance and audit

We ask that you indicate whether your company has an independent compliance function and an audit function. If not, you must explain why. The *Wwft* requires that your company has these functions if such a requirement is proportionate to your company's nature and size. Given that providing crypto services involves high risks, we are working on the assumption that your company has both an independent compliance function and an audit function.

We would also like to receive a description of the following:

- procedures in place to ensure that detected deficiencies or shortcomings are reported to the appropriate individuals
- procedures in place to ensure that detected deficiencies or shortcomings relating to ethical operational management are appropriately remedied under the supervision of the compliance function.

Please note that 'independent' means that relatives or shareholders cannot fulfil this function. Most companies have also specified this in their regulations on conflicts of interest. If you have any doubts about your company's governance structure, you have the option of discussing this with us prior to registration.

5.3 Reporting procedure

The law requires that crypto service providers have arrangements in place that allow staff members or individuals in comparable positions to report breaches of the *Wwft*. We ask that you describe this procedure.

5.4 Outsourcing

We must be able to supervise your company, also if it outsources certain activities that are related to the *Wwft* and the *Sw*. This is why we ask that you describe which activities your company outsources, and why. Please keep in mind that certain activities related to compliance with the *Wwft* must not be outsourced. One example of such an activity is monitoring a business relationship and the transactions conducted during the existence of that relationship on an ongoing basis, to ensure that they match your company's knowledge of the customer and the customer's risk profile. Please provide the outsourcing agreements for activities that relate to compliance with the *Wwft* and the *Sw*.

5.5 Education and training

Adequate implementation of processes and procedures largely depends on the level of knowledge and experience of staff members. This is why knowledge and experience of risk management (including money laundering and terrorist financing) are important preconditions for developing an adequate control framework. Educating and training staff is an important tool to communicate and anchor knowledge within your company about the *Wwft* and the *Sw* and about the principles and procedures of your company's integrity policy.

Your company must offer its staff members training programmes to ensure that they are acquainted with the provisions of the *Wwft* and the *Sw*, to enable them to perform customer due diligence fully and correctly and to identify unusual transactions. These programmes should focus on money laundering and terrorist financing techniques, methods and trends, on the international context and standards, and on new developments in this area. To enable your staff members to keep abreast of new developments and to improve awareness in the long term, your company must provide training programmes at regular intervals and at different levels, rather than as one-off sessions. The compliance function is also advised to attend additional training programmes to keep up to date on new developments in national and international legislation and regulations, and risks of money laundering and terrorist financing.

6 Ethical business operations

The integrity of your company is a precondition for its proper functioning. It is essential that you prevent your company from becoming involved in unlawful acts. Managing integrity risks is the pivotal issue here. Integrity risks include money laundering and terrorist financing.

Your company must pursue an adequate integrity policy to ensure ethical operational management. This integrity policy must be detailed and implemented in clear and readily accessible procedures and measures, documented, for instance, in a procedures manual.

The regulatory framework for an adequate integrity policy is risk-based, meaning that your company must implement all measures that the law requires. The focus of these measures depends on the risks that your company is specifically exposed to. These measures may for instance be related to the nature and background of customers, the type of product or service provided, the combination of customer and product, and how your company maintains its customer contacts. Providing crypto services involves high integrity risks, meaning that more measures will most likely be needed in your sector compared with other sectors that must comply with the *Wwft* and the *Sw*.

You must assess the risks that your company is exposed to and formulate sufficient mitigating measures. The framework of the *Wwft* assumes that a company classifies its customers by risk categories, based on the nature and size of its risk exposure. These risk categories vary from low to high risk, and classification should be based on objective and identifiable indicators. The higher the risks, the more efforts your company should make to mitigate them. You must also indicate which risks you find unacceptable.

The following elements must at least be discussed:
- an analysis of integrity risks
- avoiding conflicts of interest;
- customer due diligence
- Sanctions Act 1977 (Sw)
- transaction monitoring
- obligation to report unusual transactions
- designation of a day-to-day policymaker who bears responsibility for compliance with the *Wwft* and the *Sw*.

Below, we describe these elements in further detail.

6.1 Analysis of integrity risks

This integrity risk is systematic, which is why we use the acronym SIRA. It is a tool for ensuring ethical operational management.

As risks change continuously, the SIRA has a sell-by date, i.e. a date by which the analysis must be updated. At a minimum, the SIRA which we will consider together with your request for registration must be up to date. It must also describe the situations in which elements of the analysis need repeated or supplementary review, or when the review must be brought forward.

The analysis must be verifiable, i.e. recorded in a separate document, and the integrity policy must be based on the outcome of the SIRA. Your company must use a comprehensible quantification method. The SIRA is based on gross (inherent) and net (residual) risks and analyses the likelihood and impact of these risks. The size of net risks must be clear and the measures and procedures must have a plausible effect.

The SIRA must at least include an analysis of the following risks: money laundering and terrorist financing, non-compliance with sanctions legislation, and other risks related to ethical operational management, such as conflicts of interests and corruption. It must also include an analysis of risks associated with the products and services provided to customers. This analysis must be used in drawing up the customer profiles used. Your company must also pay extra attention to on-line customer acceptance, if applicable. This always involves a high risk and the analysis must show how your company intends to offset this elevated risk. The SIRA must also address such topics as outsourcing and risks related to the use of specific tooling in customer due diligence and transaction monitoring.

Your procedures and measures must be verifiably connected with the specific risks identified in the SIRA. The control measures set out in the SIRA must be in line with the nature, size, complexity and risk profile of your company's operations.

You will find more information on the SIRA in our user manual for producing an adequate SIRA: "Integrity risk analysis: more where necessary, less where possible" (http://www.toezicht.dnb.nl/en/binaries/50-234068.pdf)

6.2 Preventing conflicts of business and private interests

Actual or perceived conflicts of interest may negatively affect your company as well as its customers. Your company must have procedures and measures in place to prevent conflicts of interests of policymakers, group directors, supervisory board members and other staff members or individuals who permanently work for the company.

This policy should make clear how you approach:

- personal, professional, and financial interests in relation to contacts with customers and other stakeholders
- handling information in general and confidential information
- customer relationship management
- private financial transactions
- secondary activities

6.3 Customer due diligence

You are not permitted to start providing services to customers before you have identified and verified the customer and the ultimate beneficial owner (UBO), by means of customer due diligence. You must therefore clearly explain the procedures and measures contained in the customer due diligence exercise. Procedures and measures relating to client acceptance must be in accordance with your company's integrity policy, the outcome of the risk analysis and statutory requirements in the *Wwft* and the *Sw*.

When performing customer due diligence, you must take account of the following points.

- Your company must verify the identity of all customers based on independent and reliable documents.
- Your company must be sufficiently familiar with the customer's or legal entity's ownership and control structure.
- Your company must be well aware of, and must have adequately documented, why and with what intention the customer wants to use your company's services, and it must see to it that this is incorporated into the customer's risk profile.
- The company must keep all such information in readily accessible form for at least five years after it has ceased providing services to or terminated its business relationship with the customer in question. Please note that this also applies to companies that have terminated their activities and/or are no longer registered.
- All customer data and files relating to the customer and the ultimate beneficial owner must be kept in a central place accessible to compliance officers and other relevant staff members.

Procedures and measures must document how and by whom customer due diligence is to be performed. The relevant staff members must be made aware of the internal and statutory requirements imposed on customer due diligence. Customer acceptance must be approved by authorised staff members or management based on the four-eyes principle. Business relationships with certain types of customers require the explicit approval of senior management.

Your company must also record when enhanced customer due diligence is required and which measures it intends to take in such cases, and document whether customers or UBOs are politically exposed persons (PEPs). Your company must assign its customers, products and services to risk categories and state the reasons for allocating them to these specific categories. This classification must be adequate and in line with the SIRA mentioned above. Customers must be accepted subject to screening against sanctions lists, PEP lists and any other relevant lists. Your company must record positive matches in the relevant customer file and take action where needed. These matches must also be mentioned in the customer's risk profile and must be reported to us. And finally, an exit policy must be put in place for customers who cannot or do not want to be identified, or whose identity cannot be verified in the prescribed manner. When such cases occur, they must be verifiably followed up.

We offer crypto service providers more guidance on our Open Book on Supervision web pages: https://www.toezicht.dnb.nl/en/2/50-237993.jsp, and in our "DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Act" and the Sanctions Act": https://www.toezicht.dnb.nl/en/binaries/51-212353.pdf.

6.4 Sanctions Act

You must have documentation in place setting out your policy and procedures on compliance with sanctions legislation. These procedures must guarantee the existence of a comprehensive and up-to-date inventory of services provided, broken down by countries, natural persons, legal entities and groups governed by sanctions legislation. You must also have a procedure in place for the receipt and internal distribution of sanctions lists (at least with respect to the Netherlands sanctions lists and the EU regulations).

These procedures and measures must stipulate that before providing services and thereafter on a regular basis you check relations, amongst which clients and UBO's, for matches with relations included in national and international sanctions lists (these lists are updated on an ongoing basis). Compliance with sanctions legislations also means that institutions must check incoming and outgoing transactions, and block and report them to DNB in the event of a hit. Your procedures and measures must comply with the standards and objectives of the different sanctions regulations. The procedures and measures must be structured to ensure that if a match is detected financial assets may be frozen, or financial resources or services can be prevented from becoming available to persons or entities mentioned on the sanctions list. Your company must have adequate measures in place to guarantee that any matches are reported without delay to the responsible central person or department and, if acknowledged as a match, reported to DNB.

We offer crypto service providers more guidance on our Open Book on Supervision web pages: https://www.toezicht.dnb.nl/en/2/50-237993.jsp and https://www.toezicht.dnb.nl/en/2/50-237925.jsp, and in our "DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act": https://www.toezicht.dnb.nl/en/binaries/51-212353.pdf.

6.5 Transaction monitoring and reporting of unusual transactions

Your company must have procedures and processes in place to ensure the monitoring of customer accounts, activities and transactions. This helps the company gain and retain insight into the nature and background of customers and their transaction behaviour, and detect unusual transaction patterns and transactions that by their nature entail increased risk of money laundering or terrorist financing.

Your company must have procedures and processes in place stipulating how transactions are monitored and how to act if transactions are made that may qualify as unusual, and it must make motivated and appropriate choices between electronic monitoring and manual monitoring. If there are large numbers of transactions, electronic monitoring will be the obvious choice, but this stops at detecting possible unusual transactions. Suspected unusual transactions detected during automated transaction monitoring must not be performed before they have been manually checked against the *Sw*. Procedural descriptions must state which staff members are authorised to perform manual checks, and what decision-making structure is used with respect to checking *Sw* compliance.

The company's policy and procedures must also describe how unusual transactions are reported to the Netherlands Financial Intelligence Unit (FIU-NL) immediately after they were found to be unusual. Your company must notify all relevant business units of the policies, procedures and measures relating to all subjects described above.

We offer crypto service providers more guidance on our Open Book on Supervision web pages: https://www.toezicht.dnb.nl/en/2/50-237993.jsp, and in our "DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act" and the Sanctions Act": https://www.toezicht.dnb.nl/en/binaries/51-212353.pdf.

6.6 Responsible policymaker under the *Wwft*

On the basis of Section 2d(1) of the *Wwft* an institution with two or more policymakers must appoint a management board member as its day-to-day policymaker who is responsible for compliance with the *Wwft*. This policymaker is essentially responsible for ensuring *Wwft* compliance. The responsible policymaker under the *Wwft* must at all times be fully aware of the company's integrity policy and procedures and actively monitor compliance with the relevant regulations. Last but not least, the responsible policymaker under the *Wwft* must demonstrably attend relevant education and training.

Annex – overview of the documents required for the application for registration

Below is a list of the documents required in each part of the registration form. The procedures regarding sound operational management and ethical business operations can also be bundled in a single procedures manual. The Digital Portal requires that for each topic in the registration form the relevant documentation is bundled.

Please note that this list is not exhaustive and that it does not provide a detailed overview of all the questions and explanations included in the registration form.
The documents submitted must be complete and clearly structured to ensure a smooth and successful processing of your request for registration.

Company details

- Recent extract from the Trade Register of the Chamber of Commerce of the company
- A certified copy of the company's articles of association
- A copy of the company's up-to-date shareholders' register
- Signatory statement

Business plan

- Business plan (including a schematic overview of the company's activities and strategy)

Governance

- Organisational structure (including an organisation chart)
- Description of transparent control structure

Sound operational management

- Description of the company's independent compliance function and audit function
- Reporting procedure for Wwft incidents
- Policy for outsourcing activities that are related to the *Wwft* and the *Sw*
- Copies of any outsourcing agreements that are relevant in the context of compliance with the *Wwft* and the *Sw*
- Education and training policy

20

Ethical operational management

- Systematic integrity risk analysis (SIRA)
- Integrity policy

- Policy regarding the prevention of conflicts of interest
- Description of the company's procedure to prevent conflicts of interest
- Customer due diligence policy
- Description of the company's customer due diligence procedure

- Sanctions screening policy
- Description of the company's sanctions screening procedure

- Policy for transaction monitoring and reporting of unusual transactions
- Description of the company's procedures for transaction monitoring and reporting of unusual transactions

You must submit the documents required for fit and proper assessments in the context of registration as a crypto service provider separately, with the relevant Initial assessment crypto service provider forms.

DRAFT

DeNederlandscheBank
EUROSYSTEEM

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 20 524 91 11
dnb.nl