www.coe.int/cybercrime

12 December 2024 T-CY (2024)10

Cybercrime Convention Committee (T-CY)

Virtual assets and the relevance of the Convention on Cybercrime and its Second Protocol

Questionnaire on practices by Parties to the Convention

Adopted by the 31st Plenary of the T-CY
(11-12 December 2024)

Background and purpose

The 30th Plenary Meeting of the T-CY (June 2024) decided:

- To invite the T-CY Bureau to present the T-CY plenary with possible options for future work of the T-CY on the question of virtual currencies and the relevance of the Convention on Cybercrime and its Second Protocol for criminal investigations, the collection of evidence, the search, seizure and confiscation of assets, and the cooperation with virtual asset service providers (VASPs) related to offences involving virtual assets.
- To invite the T-CY Secretariat and C-PROC to undertake preparatory work in this respect, such as a mapping of current practices, that may assist the T-CY Bureau.

In view of mapping current practices of the Parties related to virtual assets and in particular the relevance of the Convention on Cybercrime and its Second Protocol in this context, the 31st T-CY Plenary adopted the present questionnaire in December 2024.

T-CY members are invited to prepare consolidated replies to this questionnaire in cooperation with the respective authorities of their State[1] and return them to the T-CY Secretariat by 28 February 2025 to **T-CY.secretariat@coe.int**

[1] T-CY Members are encouraged to coordinate their response with their domestic authorities responsible for implementation of the FATF Recommendations.

Questionnaire

A. Definitions / concepts

Q 1: Are virtual assets (e.g. cryptocurrencies, non-fungible tokens, gaming tokens, governance tokens, etc.) defined in your domestic criminal law[2]/case law? If so, are they considered to be "computer data"[3], "property" or both, or other? Please describe.

Q 2: Are virtual asset service providers (VASPs, e.g. crypto currency businesses, crypto asset exchange providers, non-fungible token trading sites, crypto ATM operators, wallet custodians, etc.) defined in your domestic law? If so, are they also considered service providers[4]?

Q 3: Are VASPs subject to AML/CFT regulations[5]? Are all categories of VASPs, as defined by the FATF, subject to AML/CFT regulations? Has your country implemented the requirements of FATF Recommendation 15[6] with respect to VASPs[7]?

Q 4: Could the following information constitute subscriber information in the meaning of the Convention on Cybercrime[8] with respect to users of VASP services (in answering the question please provide practical examples):

- Information that leads to the identification and verification of the identity of the customer and the beneficial owner when performing the customer due diligence measures pursuant to FATF Recommendation 10.[9]
- Information accompanying all cross-border qualifying wire transfers[10] that should according to FATF Recommendation 16 always contain:
  (a) the name of the originator;
  (b) the originator account number where such an account is used to process the transaction;
  (c) the originator's address, or national identity number, or customer identification number, or date and place of birth;
  (d) the name of the beneficiary; and
  (e) the beneficiary account number where such an account is used to process the transaction.

[2] For the purposes of this questionnaire, the domestic criminal law framework is of primary importance, while the domestic civil law classification should be secondary.
[3] "Computer data" is defined in Art. 1.b. of the Convention on Cybercrime.
[4] "Service provider" is defined in Art. 1.c. of the Convention on Cybercrime.
[5] Anti-Money Laundering/Counter Terrorism Financing regulations.
In 2019, the Financial Action Task Force (FATF) extended the scope of anti-money laundering and counter-financing of terrorism (AML/CFT) measures to cover virtual assets and virtual asset service providers (VASPs). See FATF Recommendation 15 and FATF (2024), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs (fatf-gafi.org).
[6] Recommendation 15 extends the broader FATF requirements to VASPs, including but not limited to record keeping obligations (Recommendation 15 and indirectly Recommendations 10 and 11) and 'travel rule' that applies the payment transparency requirements (FATF Recommendation 15 and indirectly Recommendation 16. The travel rule requires VASPs and financial institutions to obtain, hold, and transmit specific originator and beneficiary information immediately and securely when transferring VAs).
[7] See for example, the Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity: VACG ROADMAP: JURISDICTIONS WITH MATERIALLY IMPORTANT VIRTUAL ASSET ACTIVITY (fatf-gafi.org).
[8] "Subscriber information" is defined in Art. 18.3. of the Convention on Cybercrime.
[9] See Interpretive note to FATF Recommendation 10.
[10] Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. See Interpretive note to FATF Recommendation 16.

B. Use of criminal procedure powers to obtain evidence from VASPs

Q 5: To what extent are you able to apply procedural powers (similar to those of the Convention on Cybercrime) for obtaining data from VASPs? For each applicable power, please provide details or examples of the types of evidence relating to a virtual asset sought.

- Orders for data preservation (similar to Articles 16 and 17 Convention on Cybercrime)
- Production orders (Article 18)
- Search and seizure (Article 19[11])
- Real-time collection of traffic data (Article 20)
- Interception of content data (Article 21)
- Disclosure of subscriber information (Article 7 of the Second Protocol).

Q 6: What other legal provisions and procedures do you apply for the search, seizure and confiscation of virtual assets at domestic level (legal basis, seizure process, custodial management of the seized virtual assets, confiscation procedure)? Please provide practical examples if available.

C. International co-operation

Q 7: Do you use the tools offered by the Convention on Cybercrime as legal basis for requesting data from VASPs in other Parties to this Convention?

Q 8: If so, please indicate which of the tools of Articles 29-34 of the Convention on Cybercrime are used and which tools of the Second Protocol could be used, and what types of evidence relating to a virtual asset could be requested.

Q 9: Do you use the 24/7 Network when requesting data from VASPs located in other Parties to the Convention on Cybercrime?

Q 10: What other international agreements and legal frameworks do you use for cooperation with VASPs outside your jurisdictions?

Q 11: What other international agreements and legal frameworks do you apply for the search, seizure and confiscation of virtual assets at international level (legal basis, seizure process, custodial management of the seized virtual assets, confiscation procedure)?

Q 12: Do you use voluntary cooperation mechanisms when requesting data from VASPs outside your jurisdiction?

Q 13: Are you aware of specific channels, portals or platforms provided by VASPs to facilitate their cooperation with law enforcement authorities?

D. Legal challenges

Q 14: Can you summarise the main legal challenges encountered when seeking to obtain information or evidence (a) from VASPs within your territory and (b) from VASPs located outside your jurisdiction, and how do you overcome them?[12]

Q 15: Approximately how long does it take VASPs to comply with requests/orders?

[11] Are your authorities empowered to apply all elements of Art. 19, including its paragraph 3, letters a-d of the Convention (seizure or similar securing of computer data accessed) in relation to virtual assets?

[12] Legal challenges may relate to the application of the procedural powers and international cooperation provisions of the Convention on Cybercrime or other legal challenges to the application of the criminal law framework.

Resources:

Council of Europe/MONEYVAL report:

- https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4
- Convention on Cybercrime (ETS 185)
- Second Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS 224)

FATF reports:

- https://www.fatf-gafi.org/en/topics/virtual-assets.html
- https://www.fatf-gafi.org/en/publications/Virtualassets/VACG-Snapshot-Jurisdictions.html
- FATF Recommendations