April 20th, 2021

Comments of CGTF on the draft revised VASP Guidance

Dear FATF team,

We appreciate a strenuous effort by national regulators and authorities to work with standards for virtual assets and its providers.

We are hereby providing an input to the FATF draft guidance on a risk-based approach to VAs and VASPs.

About Cryptoassets Governance Task Force[1]

Cryptoassets Governance Task Force (CGTF) is a Japan-based non-profit community which provides technical information (e.g., security) for cryptoassets in multi-stakeholder approach including academia, technical community, and private sector entities established in Feb. 2018.
Since establishment, CGTF worked to develop a security consideration on risk management for virtual assets for consumer and investor protection prior to the discussion by regulators and self-regulatory organization.

The security consideration on cryptoasset custodians (in Japanese[2]) is published as the result of broad discussion with an engagement of academia ,technical communities, and VASPs. We published the documents as proposed standards at international standardization body (IETF[34]) to build a shared understanding of risk about virtual assets.

With those activities, we established a cooperative relationship with a self-regulation organization (Japan Virtual and Crypto assets Exchange Association[5]).

[1] https://vcgtf.github.io/

[2]暗号資産カストディアンのセキュリティ対策についての考え方（案）(in Japanese)

[3] Sato, M., Shimaoka, M., and Nakajima, H., "General Security Considerations for Cryptoassets Custodians", draft-vcgtf-crypto-assets-security-considerations-07 (work in progress), December 2020.

[4] Nakajima, H., Kusunoki, M., Hida, K., Suga, Y., and T.Hayashi, "Terminology for Crypto Asset", draft-nakajima-crypto-asset-terminology-05 (work in progress), December 2020.

[5] https//jvcea.or.jp/

Comments

Focus Area 1

Does the revised Guidance on the definition of VASP (paragraphs 47-79) provide more clarity on which businesses are undertaking VASP activities and are subject to the FATF Standards?

We think further guidance is needed on how the FATF Standards apply to various business models, and the following clarifications will help FATF requirements to be implemented smoothly.

Paragraph.42

> Firstly, VAs must be digital, and must themselves be digitally traded or transferred and be capable of being used for payment or **investment purposes**. That is, they cannot be merely digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations, without an inherent ability themselves to be electronically traded or transferred and the possibility to be used for payment or investment purposes.

Clarify what is meant by "investment purposes" in this context.
Since any asset or product can have capital gains, the interpretation of "investment" may lead to a larger scope than necessary. In order to prevent regulatory arbitrage, please define a certain scope, such as an investment contract.

Paragraph.55

> Where custodians need keys held by others to carry out transactions, these custodians still have control of the asset. ~~**A user, for example, who owns a VA, but cannot send it without the participation of others in a multisignature transaction, likely still controls it for the purposes of this definition.**~~ Service providers who cannot complete transactions without a key held by another party are not disqualified from falling under the definition of a VASP, regardless of the numbers, controlling power and any other properties of the involved parties of the signature. The limb is conceptually similar to what Recommendation 14 on money and value transfer services (MVTS) covers for traditional financial assets. An example of a service covered by (iii) includes the function of facilitating or allowing users to send VAs to other individuals, as in a personal remittance payment, payment for nonfinancial goods or services, or payment of wages. A provider offering such a service will likely be a VASP.

Please delete this unnecessary sentence because: the definition of Limb (iii) is already clearly explained by the preceding and following sentences; and this is misleading since the "user" seems to be included in the definition of VASP.

Paragraph.60

> Limb (iv) of the VASP definition should also be read expansively. Any entity that provides or facilitates control of assets or governs their use may qualify under part (iv) as this is the conceptual meaning of the words “administration” and “safekeeping”. **In simplest terms, “safekeeping” consists of the service of holding a VA or the private keys to the VA on behalf of a customer. As in the definition of “transfer”, this would include circumstances where keys or credentials held by others are required in order to change the assets disposition, such as multisignature processes.** In order to further clarify, “administration” could also include the concept of “management.”

Service providers that just follow instructions from VASPs may not need to be included in the definition of VASPs, even if they may hold keys. This is because such service providers may only be providing the infrastructure for the transaction. Or such a service provider may only help other VASPs to transfer VAs. If a VASP mitigates the ML/FT risk of a transaction, the service provider helping the VASP may not need to fulfill any obligations as VASPs, even if the service provider signs the transaction with a private key.
To hold any private keys does not mean the holders face any ML/TF risk. There may be service providers with various forms of key holding and multisignature usage, as described below.
Please clarify cases where obligations as VASPs are not required. It is possible that the obligations as VASPs should not be general. There may be some cases that some service providers of VASPs cannot do their part.

1. **Service providers with vaults of the private keys.** There would be private keys in the facilities of service providers such as cloud services and data centers, a part of these providers set an option about vaults service with special equipments including software/hardware HSM.nly the VASP as a provider’s customer has access to the private keys and can use them under control from outside. In such cases, it should be clear that any service providers such as data centers providers or cloud service providers are not VASPs. Note that these service providers should not be in a position to know the VASPs’ customers or where their VAs are transferred.
2. **Service providers that are outsourced by VASPs to verify transactions signed by VASPs and make additional signatures.** Such service providers are used by VASPs to prevent unauthorized signatures and/or unauthorized transfer of VAs due to VASP's own carelessness, system failures, leakage of private keys, or internal crimes. Such service providers will sign the transactions created by the VASPs. Since the VASPs have already fulfilled their obligations as a VASPs, the ML/FT risk of the transactions have already been mitigated. Such service providers that always transfer VAs with the cooperation of VASPs would not need to fulfill the overlapping obligations of VASPs. In addition, such service providers are not in a position to know directly the VASP's customers or the people to whom their VAs are transferred. If regulations do not anticipate such service providers and make it difficult for such service providers to do business, it may reduce the security of VASPs that were maintained by the use of such service providers.
3. **A Service provider that acts as an escrow for the buyer and seller who settle by VAs using a smart contract.** For example, first the buyer locks the VAs into the smart contract, and then the locked VAs are transferred to the seller when the service provider writes into the smart contract that the contract has been completed. If the

service provider writes that the contract has been cancelled, the VAs will be returned to the buyer. All the service provider has to do is to record the completion or cancellation of the contract into the smart contract. The service provider cannot freeze the assets or transfer the VAs to anyone except the seller and buyer. When the service provider does not do anything, the VAs will be transferred to the default recipient (buyer or seller). Are there any needs to regulate such service providers as VASPs that can only write the result of contracts into smart contracts ?

4. **A Service provider that is required for a user (owner of the VAs) to transfer VAs.** For example, a user has one key, and a service provider has another key. The transfer of VAs requires the signing of both the user and the service provider keys. The user cannot transfer the VAs unless the service provider signs it. Such service providers can mitigate ML/TF risk by fulfilling its obligations as a VASP.
5. **A Service provider with a private key that is not required for a user (owner of the VAs) to transfer VAs.** In a multisignature wallet, where a user has two keys himself and a service provider has one key for the user, the design may be such that the user can transfer VAs with only the two keys that he controls. When the user alone transfers the assets, the service provider has no opportunity to fulfill its obligations as VASPs. Such a service provider can be used, for example, to ensure that a user will not lose the ability to move assets if he loses one of his own keys. In other cases, it may be used for the purpose that the user keeps one of his own keys strictly as a backup and uses the other user's key and the service provider's key for routine transfer of VAs.
6. **A Service provider that can transfer VAs without a user (owner of the VAs) in a circumstance where the user can also transfer VAs without the service provider.** VAs can be transferred by the user without the service provider, and the service provider without the user. The service provider cannot stop the user from transferring VAs.

Paragraph.70

> Just as the FATF does not seek to regulate the individual users (not acting as a business) of VAs as VASPs—though recognizing that such users may still be subject to compliance obligations under a jurisdiction’s sanctions or enforcement framework—the FATF similarly does not seek to capture the types of closed-loop items that are non-transferable, non-exchangeable, and non-fungible. Such items might include airline miles, credit card awards, or similar loyalty program rewards or points, which an individual cannot sell onward in a secondary market outside of the closed-loop system. Rather, the VA and VASP definitions are intended to capture specific financial activities and operations (i.e., transfer, exchange, safekeeping and administration, issuance, etc.) and assets that are **convertible or interchangeable**—whether virtual-to-virtual, virtual-to-fiat or fiat-to-virtual. The acceptance of VAs as payment for goods and services, as in the acceptance of VA by a merchant when effecting purchase of goods, for instance, also does not constitute a VASP activity. A service that facilitates companies accepting VA as payment would, however, be a VASP.

Clarify what is meant by “convertible or interchangeable” in this context. Even if a token has no value to many people, it could be converted to VAs or fiats at any price if the buyer and the seller are matched, so the interpretation of "convertible or interchangeable" may lead to a larger scope than necessary. To prevent regulatory arbitrage, please limit the scope to cases where the market price is such that anyone can be expected to buy or sell at approximately the same price, or where there is sufficient liquidity, as an example.

Focus Area 3

Does the revised Guidance in relation to the travel rule need further clarity (paragraphs 152-180 and 256-267)?

Paragraph.170

> Countries should require VASPs or other obliged entities to implement an effective control framework to ensure that they can comply with their targeted financial sanction obligations. This framework should take into account the nature of VA transfers. Because the required information identifying the originator and beneficiary can be held separately to the VA transfer system (e.g., the blockchain), the VA transfer can be completed even with such information missing or without screening the transfer to identify suspicious and prohibited transactions. Therefore, VASPs or other obliged entities should screen required VA transfer information separately to such direct settlement. **Thus, VASPs should consider remediation measures that fit their business process and the technical nature of VAs. Although blockchain technology is ever-changing**, examples of controls that a VASP or other obliged entity could implement include:
>
> a. put a customer wallet on hold until screening is completed and confirmed that no concern is raised; and
> b. **arrange to receive a VA transfer with a provider's wallet that links to a customer wallet.** Move the transferred VA to their customer's wallet only after the screening is completed and confirmed no concern is raised.

Some VASPs may need sufficient period for the system implementation in practice even though VASP can temporarily hold deposits and screen users technically on receiving VAs by assigning address(es) for each user, due to the following two reasons:

1. VASPs may have systems difficult to allocate a cold wallet to each user. They may need enough time to modify their systems. If there is not enough time to modify the system, the amount of VAs could be managed in hot wallets. As the amount of VAs managed by a hot wallet increases, it becomes less secure than a cold wallet.
2. It may affect the cost to modify systems, train operators, and inform users.

Paragraph.173

> The best way to conduct counterparty due diligence in a timely and secure manner is a challenge. There are broadly three phases in this process:
>
> a) Phase 1: Determine whether the VA transfer is with a counterparty VASP. A customer may wish to transfer VAs to another VASP (e.g., a beneficiary with a hosted wallet) or they may wish to transfer VAs to an unhosted wallet. The originator VASP must therefore determine whether they will be transacting with another VASP. This determination process is not purely an AML/CFT requirement, but rather arises from the technology underpinning VAs. To date, the FATF is not aware of any technically proven means of identifying the VASP that manages the beneficiary wallet exhaustively, precisely, and accurately in all circumstances and from the VA address alone;
>
> b) Phase 2: Identify the counterparty VASP, as a VASP only knows the “name” of the counterparty VASP following the previous phase. A VASP may identify a counterparty VASP themselves **using a reliable database in line with any guidelines from a country on when to rely on such data; and**
>
> c) Phase 3: Assess a counterparty VASP if they are an eligible counterparty to send customer data to and to have a business relationship with (see Recommendation 16 in Section IV for further information on counterparty VASP due diligence and Recommendation 11 on record-keeping to appropriately store and manage that customer data).

For efficient operations of Phase 2 , request coordination and collaboration among countries to create a reliable database.

Paragraph.177

> Given the ‘sunrise issue’ in relation to the travel rule, countries should adopt a riskbased approach in the assessment of the business models presented by VASPs. Countries should consider the full context of travel rule compliance, including whether there are sufficient risk mitigation measures taken by the VASP to adequately manage the attendant ML/TF risks. Regardless of the regulation in a certain country, a VASP may implement robust control measures to comply with the travel rule requirements. Examples include VASPs restricting VA transfers to within their customer base (i.e., internal transfers of VAs within the same VASP), **only allowing confirmed first-party transfers outside of their customer base (i.e., the originator and the beneficiary are confirmed to be the same person)** and enhanced monitoring of transactions. The absence of relevant regulations in one country does not necessarily preclude the effectiveness of measures introduced by a VASP on its own.

A technical approach to achieving this would be, for example, a VASP has users create unhosted wallets on their mobile devices using the official application software published by the VASP. If the VASP has the users use those unhosted wallets, the VASP can verify that the originator and the beneficiary are the same customer.