KeySecure

SPECIFIC TERMS & CONDITIONS

Version. 20250620v1.0

KEYSECURE MPC SELF-CUSTODY

This Specific Terms and Conditions ("STC"), the General Terms and Condition ("Terms") and the Order Form (collectively the "Purchase") are deemed as part of the terms and conditions to govern the contractual relationship between You and KEYSECURE. It shall be effective between You and KEYSECURE from Effective Date upon Your signing and execution of the Order Form to purchase the KEYSECURE MPC Self-Custody. This STC does not require any signing.

Introduction

1. KEYSECURE provides customers with digital payment token ("DPT") custody services (the "Services") with greater security, ease of use, and scalability. After years of deep cultivation, the company is in a leading position in the industry in terms of technical professionalism and market foresight. KEYSECURE's system adopts multi-party computation ("MPC") technology to protect DPTs from hacker attacks and private key single point risk, and leverages whitelists and customizable withdrawal approval processes to increase the security level of users' accounts.

   In addition, KEYSECURE provides a full-link activity monitoring system allowing KEYSECURE to automatically monitor and record all of the transaction process from start to end, and ensure that all transactions are processed in accordance with the specified procedures. By using our custody services, you agree to be bound by these terms. If you do not agree, please do not use our services.

Eligibility

2. By using our Services, you confirm that you are at least 18 years old and have the legal capacity to enter into these terms. You also confirm that your use of our services complies with applicable laws and regulations.

Services Provided

3. Under this service, KEYSECURE will provide MPC wallets to customers, which will divide a single cryptographic key into three private key shards, each key shard holding a private set of data. Users will hold on to one key shard, while KEYSECURE will hold on to the remaining two key shards.

4. The execution of a transaction will require three key shards to sign and send the transaction. Whenever a key is required, the MPC is set in motion to confirm with all parties simultaneously whether they approve of the request. Parties will independently compute their part of the private key share(s) they hold to produce a signature, without revealing the encryption to other parties.

5. Users can provide instructions for the DPT stored in their wallet to be transmitted to another DPT wallet, as long as the user is able to authenticate the transaction using its key shard.

6. By default, the MPC wallet uses TRON Energy ("Energy") and TRON Bandwidth ("Bandwidth"), together known as "Resources", instead of traditional gas fees when processing transactions. The interaction of smart contracts requires Energy and Bandwidth, while the transfer of TRX currency only requires Bandwidth. If you do not have enough Energy or Bandwidth, TRX may be deducted to cover the cost.

   If you prefer not to use the Resources, you have the option to opt out through the wallet settings. Please review your preferences to ensure they align with your intended transaction method.

Product And Payment

7. Any purchase of service and/or product shall be in accordance to the package, version and/or any other service and/or product specification set forth and agreed in the Order Form. In the event of any

inconsistency between the Order Form, this Term and the General Terms and Condition, the Order Form shall prevail this Terms and this Terms shall prevail the General Terms and Conditions.

8. Option of main chains under your Purchase is always subject to KEYSECURE's availability of such main chain. Additional charges may be required for customization and development of additional main chain, if any.

9. Upon receipt of payment from you, you must create a merchant wallet account on our portal the same day to allow us to provision the KEYSECURE MPC Self-Custody wallet under.

10. 'Product Subscription Period' and/or its applicable Minimum Fee shall always commence from the when the service is first provided, unless stated otherwise.

11. Upon signing of the Order Form, you hereby confirm your possession of one key shard. You also acknowledge that any digital assets, tokens, or cryptocurrencies stored in your wallet may become irrecoverable or inaccessible in the event of loss, misplacement, or theft of your key shard. KEYSECURE shall bear no responsibility or liability whatsoever in the event of loss, misplacement, or theft of the key shard. You are responsible for obtaining your own insurance to indemnify against any loss of digital assets, tokens, or cryptocurrencies stored in your wallet.

Account Creation And Maintenance

12. To use our services, you must create an account by providing accurate and complete information. You are responsible for maintaining the confidentiality of your account credentials and for all activities that occur under your account. You shall notify us immediately if you notice any unauthorized use of your account.

13. Whenever a customer requests any action of KEYSECURE, it will be required to provide its instructions. KEYSECURE acts upon instructions given by its customers or any person authorised by its customers to give instructions to it or perform other operations through KEYSECURE's website on behalf of its customers ("Authorised Persons") that are received and verified by KEYSECURE pursuant to this Purchase. Any instructions given will continue in full force and effect until cancelled (if possible) or executed.

14. The customer is required to maintain an updated and current list of Authorised Persons at all times with KEYSECURE and will immediately notify KEYSECURE of any changes to the list of Authorised Persons by updating the list on the platform, including for termination of employment, or otherwise. The customer shall make available all necessary documentation and identification information, as reasonably requested by KEYSECURE to confirm:

a. the identify of each Authorised Person;

b. that each Authorised Person is eligible to be deemed an "Authorised Person" as defined above; and

c. that the person(s) requesting the changes in the list of Authorised Persons have valid authority to request changes on behalf of the customer.

15. KEYSECURE shall be entitled to rely upon any instructions it receives from an Authorised Person (or from a person reasonably believed by KEYSECURE to be an Authorised Person) in accordance with this Purchase. KEYSECURE may assume that any instructions received from a customer or Authorised Person are not in any way inconsistent with the provisions of organisational documents of the customer or of any vote, resolution, or proper authorisation and that the customer is authorised to take the actions specified in the instructions.

16. The customer must verify all transaction information prior to submitting instructions to KEYSECURE. KEYSECURE shall have no duty to inquire into or investigate the validity, accuracy or content of any instructions. If any instructions are ambiguous, incomplete, or conflicting, KEYSECURE may refuse

to execute such instructions until any ambiguity, incompleteness, or conflict has been resolved. KEYSECURE may refuse to execute instructions if, in its sole opinion, such instructions are outside the scope of its duties under this Purchase or are contrary to any applicable laws.

17. KEYSECURE will provide customers, on a real-time basis, the following particulars in the form of electronic records stored on an electronic facility.

a. transactions to purchase or sell assets entered into by the customer and the price at which the transactions are entered into;

b. the status of every asset (including DPT) in KEYSECURE's custody held for the customer, including any asset (including DPT) deposited with a safeguarding person (if any);

c. the movement of every asset (including DPT) of the customer, the date of and reasons for such movement, and the amount of the asset (including DPT) involved;

d. the movement and balance of relevant money received from, or on account of, the customer in respect of the provision of the Services (if any); and

e. a detailed account of all financial charges and credits to the customer's account during the monthly statement period, unless the detailed account of financial charges and credits has been included in any contract note or tax invoice issued by KEYSECURE to the customer.

18. By using our Services, you consent to the particulars above being made available to you in this manner and the above shall suffice as the provision of a statement of account, and you consent to not receive any separate statement of account from KEYSECURE on a monthly basis.

Security Measures

19. KEYSECURE will retain control over access to the underlying DPT in the MPC wallets it provides in the following ways –

a. KEYSECURE will hold two of the three key shards of each MPC wallet;

b. As all three key shards are required to execute a DPT transaction to or from the MPC wallet, KEYSECURE would have the ability to co-authorise a transaction by signing the two key shards it holds; and

c. KEYSECURE may, in rare circumstances (such as when transaction monitoring checks are failed) block the execution of a transaction, either by way of the KYT transaction monitoring tool or by withholding KEYSECURE's signing of the two key shards that KEYSECURE holds.

20. The MPC wallets allow for the function for users to provide instructions for the DPT stored in its MPC wallet to be transmitted to another DPT wallet, as long as the user is able to authenticate the transaction using its key shard.

21. Additionally, KEYSECURE would not only be facilitating the transfer of DPT and moving DPT from one account to another (i.e., either from a user's MPC wallet to another DPT wallet, or from another DPT wallet to a user's MPC wallet), it would also be in possession of such DPT being transferred.

22. Where appropriate, KEYSECURE uses available technology to protect the security of communications made through our KEYSECURE website. Do note that KEYSECURE do not accept liability for the security, authenticity, integrity or confidentiality of any transactions and other communications made through our KEYSECURE website. Internet communications may be susceptible to interference or interception by third parties. KEYSECURE will do our best but KEYSECURE cannot make any warranties that our KEYSECURE website is free of infection by computer viruses or any other unauthorised software.

Custody And Control

23. While KEYSECURE holds your digital assets in custody, you retain ownership and control over them. KEYSECURE will not use, lend, or leverage your assets for any purpose other than those specified in these terms or as instructed by you.

Transaction Processing

24. You may instruct us to execute transactions involving your digital assets. KEYSECURE will process these transactions in accordance with your instructions, provided they comply with our security procedures and legal requirements.

Liability

25. To the maximum extent permitted by applicable law and subject to the exceptions provided in clause 27 below, in no event shall KEYSECURE, its affiliates and service providers, or any of their respective officers, directors, agents, employers or representatives, be liable for any lost profits or any special incidental, indirect, intangible, or consequential damages, whether based in contract, tort, negligence, strict liability, or otherwise, arising out of or in connection with authorised or unauthorised use of the Services, or this Purchase, even if KEYSECURE has been advised of or knew or should have known the possibility of such damages.

26. To the maximum extent permitted by applicable law and subject to the exceptions provided in clause 27 below, in no event shall the aggregate liability of KEYSECURE, its affiliates and service providers, or any of their respective officers, directors, agents, employees or representatives, exceed the fees paid or payable to KEYSECURE under this Purchase during the 6 months period immediately preceding the first incident giving rise to such liability.

27. The exclusions and limitations of liability in clause 25 and clause 26 will not apply to KEYSECURE's fraud, wilful misconduct, or gross negligence. KEYSECURE's liability for gross negligence shall be limited to the value of the affected digital assets or fiat currency.

28. In the event of losses of customers' digital assets arising from fraud or negligence on the part of KEYSECURE, KEYSECURE will act in accordance with its compensation framework. Under this framework:

29. Customers are advised to promptly report any losses and associated suspicious activity to KEYSECURE's support team through custody@KEYSECURE.com

30. KEYSECURE will investigate the matters and endeavour to provide a resolution within 30 days. In any event, KEYSECURE will provide the affected customer with an update within this timeline;

31. As part of KEYSECURE's investigations into the matter, KEYSECURE may contact the customer and/or any other relevant third parties for further information; and

32. If the result of KEYSECURE's investigations reveal that the claim is valid, KEYSECURE will compensate the customer for any direct losses suffered by the customer in connection with KEYSECURE's fraud or negligence. Notwithstanding this, if a customer may potentially be able to make a claim under any form of insurance coverage, the customer shall not be entitled to such compensation by KEYSECURE to the extent of the sum insured.

User Obligations

33. You agree to:

a. comply with all applicable laws and regulations;

b. provide accurate and complete information;

c. keep your account credentials secure; and

d. promptly update us on any changes to your information.

Termination

34. KEYSECURE may terminate or suspend your account at our discretion if you violate these terms or if required by law. You may terminate your account by providing us with written notice. Upon termination, KEYSECURE will return your digital assets to you, subject to any outstanding obligations.

Amendments

35. KEYSECURE may amend these terms from time to time. Continued use of our services after such changes will constitute your acceptance of the amended terms.

Governing Law

36. These terms are governed by the laws of Singapore. Any dispute arising out of or in connection with this contract, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration administered by the Singapore International Arbitration Centre ("SIAC") in accordance with the Arbitration Rules of the Singapore International Arbitration Centre ("SIAC Rules") for the time being in force, which rules are deemed to be incorporated by reference in this clause. The seat of the arbitration shall be Singapore. The Tribunal shall consist of 1 arbitrator appointed by KEYSECURE. The language of the arbitration shall be English.

Contact Information

37. KEYSECURE will use commercially reasonable efforts: (i) to provide reasonable technical support to customers, by email or telephone, during KEYSECURE's normal business hours from 10am-7pm (utc + 8); (ii) to respond to support requests in a timely manner; and (iii) resolve such issues by providing updates and/or workarounds to customers (to the extent reasonably possible and practical), consistent with the severity of the issues identified in such requests and their impact on the customer's business operations.

38. If you have any questions or concerns about these Terms of Use, please contact us via our official website at https://keysecure.io/

Consumer Protection Disclosures

39. The key risks of the Services are set out below:

Digital asset custody involves various forms of assets such as cryptocurrency, digital securities, non-fungible tokens (NFTs), etc. Although custody services aim to enhance asset security and compliance, there are still a series of specific risks in this field. Thorough threat and risk assessment is key to ensuring asset security, complying with laws and regulations, and resisting potential threats. The following are the main types of risks that need to be considered in digital asset custody.

Technical risk

- Hacking attacks: Even the most advanced security systems can be subject to hacking attacks, including intrusions into trading systems, physical attacks on cold storage facilities, etc.

- System failure: Software defects, hardware failures, or data center issues can cause service interruptions and affect the availability of assets.
- Loss or leakage of private key: Secure management of private key is the core of digital asset security. Loss or leakage of private key will make related assets irretrievably lost.

Operational risk

- Internal Threats to Employees: Risk of employees abusing their access for illegal transactions or theft of assets.
- Risks of third-party service providers: Relying on third-party services (such as Cloud as a Service provider) may increase operational risks, and problems with these services may indirectly affect the security and stability of managed services.

Market risk

- Asset Volatility: The prices of cryptocurrencies and other digital assets are extremely volatile. Market crashes or sharp fluctuations can cause asset values to rapidly decline.
- Liquidity Risk: Under certain market conditions, some digital assets may be difficult to liquidate immediately.

40. KEYSECURE recognises that it is crucial to adopt effective risk mitigation strategies to address these risks to consumers. Hence, KEYSECURE has a Risk Mitigation Strategy per indicated in the following to mitigate the above risks.

Technical risk

- Multi-factor authentication: A multi-factor authentication (MFA) policy is in place to enhance account security.
- Distributed Denial of Service (DDoS) Protection: By adopting advanced DDoS mitigation tools and strategies, KEYSECURE's systems and policies are better able to protect hosted platforms from attacks.
- Regular security audits: Regular security audits and penetration testing exercises are conducted to identify and fix potential security bugs and other system vulnerabilities.

Operational risk

- Disaster Recovery Plan: KEYSECURE regularly updates its Disaster Recovery and Business Continuity Plan to ensure that managed services can quickly recover in the event of an emergency.
- Technical maintenance: Regular maintenance and upgrades of the system are in place to reduce the risk of technical failure.
- Employee training: Safety awareness and compliance training for employees are in place to reduce the risk caused by operational errors. In managing employee access to customer information, KEYSECURE applies the principles of "never alone", "segregation of duties", and "least privilege" so that no one person has access to perform sensitive system functions.

Market risk

- Diversification: KEYSECURE advises its clients to diversify their investments to reduce the impact of market volatility.
- Market monitoring: KEYSECURE closely monitors market trends and responds promptly to significant events that may affect client assets.
- Price Warning System: KEYSECURE provides a price warning system to help clients monitor and manage market fluctuations.

<u>Safeguarding Of Digital Assets</u>

41. Each customer's assets are independently held, which means that the assets of each customer will not be mixed together. They are all located at the customer's own address and are kept independently by the customer

42. Customers will receive timely notifications through our platform regarding any entitlements accruing to their digital assets. Any such entitlements will be deposited into the customer's custodial accounts held with KEYSECURE. To view and access their entitlements, customers can login to KEYSECURE's platform and navigate the same.

43. KEYSECURE's storage system uses MPC technology, multi-signature technology, and multi-authentication, combined with hardware isolation for asset project management, to protect digital assets from hacker attacks and theft. At the same time, it uses allowlist and customizable withdrawal approval process to improve account security level.

Distributed Key Storage Technology

44. KEYSECURE uses distributed key storage technology, allowing users to generate and manage all private key sharding. Among them, users save one private key locally, while the other two are stored on Amazon Cloud and Microsoft Cloud respectively in Singapore. This distributed storage method combines hardware isolation technology, allowing users to fully control their assets. KEYSECURE supports 3-3 TSS configuration; when users initiate transaction signatures, these three private key sharding will participate in the signature at the same time, eliminating the single point of failure problem in private key management and significantly improving the security of asset self-management, ensuring that users' investment assets reach the highest level of security in the market.

Full-Process Node Monitoring And Auditing

45. Users can customize trading strategies. Asset trading orders subject to risk control need to be approved by designated co-management members. Only after reaching a specific approval threshold can they enter the final signature broadcast stage. At the same time, full-process node monitoring is provided, allowing users to intuitively understand the status of trading orders at each stage, ensuring clear and complete approval flow, not only meeting internal control and financial audit needs, but also ensuring the security and credibility of transactions.

Conflicts of Interest

46. As a provider of a broad range of financial services, KEYSECURE may face actual and potential conflicts during the course of its activities. These may arise from any one or combination of the following:

a. KEYSECURE and its customer relationships;

b. KEYSECURE and any other third-party service provider duties;

c. employee interests which potentially compete with KEYSECURE products or services; and

d. potentially competing interests between two or more customers.

47. KEYSECURE utilises various means to prevent and manage conflicts of interest, which include the following:

a. employee compliance policies and directives that require disclosure, monitoring and reporting of conflicts of interest that arise involving an employee, KEYSECURE, and/or a customer;

b. clear governance rules relating to the handling and management of third-party relationships;

c. mandatory legal, risk and compliance reviews monitoring whether specific activities will give rise to conflicts of interest; and

d. provision of internal guidance and training on the handling and disclosure of conflicts of interest.

48. KEYSECURE discloses conflicts of interest in cases where it is not possible to avoid or resolve the conflict. Such disclosure is made in a clear and direct manner, using the appropriate medium.

Customer Account Setup

49. The customer agrees to provide KEYSECURE with the information KEYSECURE requests (which KEYSECURE may request at any time deemed necessary) for the purposes of identity verification and the detection of money laundering, terrorist financing, fraud, or any other financial crime, and permit KEYSECURE to keep a record of such information. The customer will need to complete certain verification procedures before the customer is permitted to start using the Services.

50. The information KEYSECURE requests may include but is not limited to personal information such as the customer's full name (including any aliases), unique identification number, residential/registered/business address, telephone number, email address, date of birth or incorporation/establishment/registration, nationality, and any such information that KEYSECURE is required to collect from time to time under applicable law.

51. The customer may also be required to undergo enhanced due diligence procedures, where KEYSECURE may request that the customer submit additional information about itself and its business, provide relevant records, and arrange for meetings with KEYSECURE's staff so that KEYSECURE may, among other things, establish the source of the customer's wealth and source of funds for any transactions carried out in the course of the customer's use of the Services.

52. In providing KEYSECURE with this or any other information that may be required, the customer confirms that the information is true, accurate and complete, and the customer has not withheld any information that may influence KEYSECURE's evaluation of the customer for the purposes of the customer's use of the Services. The customer undertakes to promptly notify in writing and provide KEYSECURE with information regarding any changes in circumstances that may cause any such information provided to become false, inaccurate or incomplete and also undertake to provide any other additional documents, records and information as may be required by KEYSECURE and/or applicable law. The customer permits KEYSECURE to keep records of such information. KEYSECURE will treat this information in accordance with applicable data protection laws.

Termination

53. In event of termination of your Purchase, it is your responsibility to withdraw all and every Assets under your Purchase. Any additional management service provided by KEYSECURE after such termination shall be borne by you and KEYSECURE is entitled to charge you additional payment at its discretion.

54. KEYSECURE shall not liable for any failure, delay, error, inaccuracy or non-compliance incurred by you during such withdrawal.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT EMPTY