Technical Paper 4
Security – Principle

Version 01

20th October, 2018

IMPORTANT: You must read the following disclaimer before continuing. This disclaimer applies to the information contained in this document and you are therefore advised to read this disclaimer carefully before reading, accessing or making any other use of the information contained in this document.

THE CONTENTS OF THIS DOCUMENT ARE CONFIDENTIAL AND ARE NOT FOR RELEASE, PUBLICATION OR DISTRIBUTION, IN WHOLE OR IN PART, DIRECTLY OR INDIRECTLY, IN OR INTO OR FROM THE UNITED STATES OF AMERICA, AUSTRALIA, CANADA, JAPAN, SOUTH AFRICA, CHINA, SOUTH KOREA OR ANY JURISDICTION WHERE SUCH RELEASE, PUBLICATION OR DISTRIBUTION IS UNLAWFUL. THIS EMAIL AND ANY ATTACHED DOCUMENTS ARE BEING SUPPLIED TO YOU SOLELY FOR YOUR INFORMATION AND DO NOT CONSTITUTE OR FORM PART OF, AND SHOULD NOT BE CONSTRUED AS, ANY OFFER FOR SALE OR SUBSCRIPTION OF, OR SOLICITATION OF ANY OFFER TO BUY OR SUBSCRIBE FOR OR OTHERWISE ACQUIRE, CRYPTOGRAPHIC TOKENS IN ANY JURISDICTION, OR AN INDUCEMENT TO ENTER INTO INVESTMENT ACTIVITY. THE CONTENTS HEREOF SHOULD NOT BE CONSTRUED AS INVESTMENT, LEGAL, TAX OR OTHER ADVICE AND YOU SHOULD CONSULT YOUR OWN ADVISERS AS TO LEGAL, BUSINESS, TAX AND

OTHER RELATED MATTERS. THERE IS NO OBLIGATION TO UPDATE THE INFORMATION CONTAINED IN THIS EMAIL OR ANY ATTACHED DOCUMENTS, AND NO REPRESENTATION OR WARRANTY IS GIVEN IN RESPECT OF THE ACCURACY OR COMPLETENESS OF SUCH INFORMATION. IF YOU HAVE ANY QUESTIONS IN RELATION TO ANY OF THE CONTENTS OF THIS EMAIL OR ANY ATTACHED DOCUMENTS PLEASE CONTACT **MR KOJI FUSA AND MR YU KUSAKABE** AT koji.fusa@gve.co.jp and yu@gve.co.jp respectively.

By accessing this document, you warrant, represent, undertake and acknowledge that (i) you have read and agreed to comply with the limitations and restrictions herein including, without limitation, the obligation to keep this email and the contents of any attached documents confidential until notified otherwise; (ii) you are able to receive this email and any attached documents without contravention of any applicable legal or regulatory restrictions; (iii) you (1) do not reside; (2) are not located; (3) do not have a place of business; and (4) are not conducting business (any of which makes a person “Resident”) in the

state of New York or in any jurisdiction in which offering, purchasing, selling, transferring or using cryptographic tokens is prohibited by any applicable statutes, laws (including common laws), ordinances, rules, regulations, codes, orders (including any temporary, preliminary or permanent order, judgment, injunction, decree, ruling or other similar event or action), and government and regulatory agency orders or guidance (collectively, "Laws"); (iv) you are not a Resident of any state or country: (1) that requires entities engaged in business, sales or offerings relating to cryptocurrency, cryptographic tokens, or crypto-databases to be registered or licensed, to seek any consent or approval, or to make any filing; or (2) where the sale or purchase of cryptographic tokens would be unlawful; (v) you are not a Resident of the United States or a "U.S. person" within the meaning of Rule 902(k) under the US Securities Act 1933; (vi) you are not a resident of, established in, or otherwise operating from a jurisdiction that is subject to country-wide or territory-wide economic, financial, or trade sanctions, which at the time of circulation of these materials includes Cuba, Iran, North Korea, Syria, and the Crimea region; and (vii) you acknowledge that you understand the legal and regulatory sanctions attached to the misuse, disclosure or improper circulation of this email and any attached documents and that any failure to comply with the restrictions herein may constitute a violation of the securities Laws of any such jurisdiction. Any person into whose possession this email or any attached documents come should inform themselves about, and observe, any such restrictions.

This document may contain certain statements and information which may constitute “forward-looking statements.” Forward-looking statements are based on our management's current expectations, contain projections of results of operations or of financial condition or forecasts of future events. Words such as “may,” “will,” “would,” “could,” “assume,” “forecast,” “position,” “predict,” “strategy,” “expect,” “intend,” “plan,” “estimate,” “anticipate,” “believe,” “project,” “budget,” “potential” or “continue,” and similar expressions are used to identify forward-looking statements. All statements that address operating performance, events, structures or developments that we expect or anticipate will occur in the future are forward-looking statements. We believe that these forward-looking statements are reasonable as and when made. They can be affected by assumptions used, or by known or unknown risks or uncertainties, some of which are beyond our control. Consequently, no forward-looking statements can be guaranteed. When considering these forward-looking statements, you should keep in mind the risk factors and other cautionary statements in this email or any documents attached to it. Actual results may vary materially. You are cautioned not to place undue reliance on any forward-looking statements. You should also understand that it is not possible to predict or identify all risk factors applicable to the information contained in this email or any documents attached to it and should not presume any such list to be a complete statement of all potential risks and uncertainties. If one or more of any such risks or uncertainties materialize, or if underlying assumptions prove incorrect, our actual results may differ materially from those anticipated, estimated, projected or expected. Each forward-looking statement speaks only as of the date of the particular statement and we undertake no obligation to update or revise any forward-looking statement, whether as a result of new information, future events or otherwise.

Security design based on the Common Criteria

- International Organization for Standardization has explained the way how to deal with the security in Information Technologies under ISO/IEC15408, called Common Criteria
- EXC Platform is designed based on ISO/IEC15408
- Our basic philosophy - to have the strongest security while expanding with existing operators - is as follows;
  1. The security design for connectivity with other platforms would become public, and
  2. The new core security feature which has various intellectual properties embedded would only be communicated with one or more of the 17 certificate authorized expert organisations.
- EXC Platform is designed to have the highest level of security by combining (1) Encryption algorithm and (2) Encryption key、and (3) Hardware security module(HSM) which aims to obtain EAL6+ under Common Criteria. Once this is complete, EXC Platform should be able to operate with purchasers of tokens able to enjoy the system with the highest level of security.

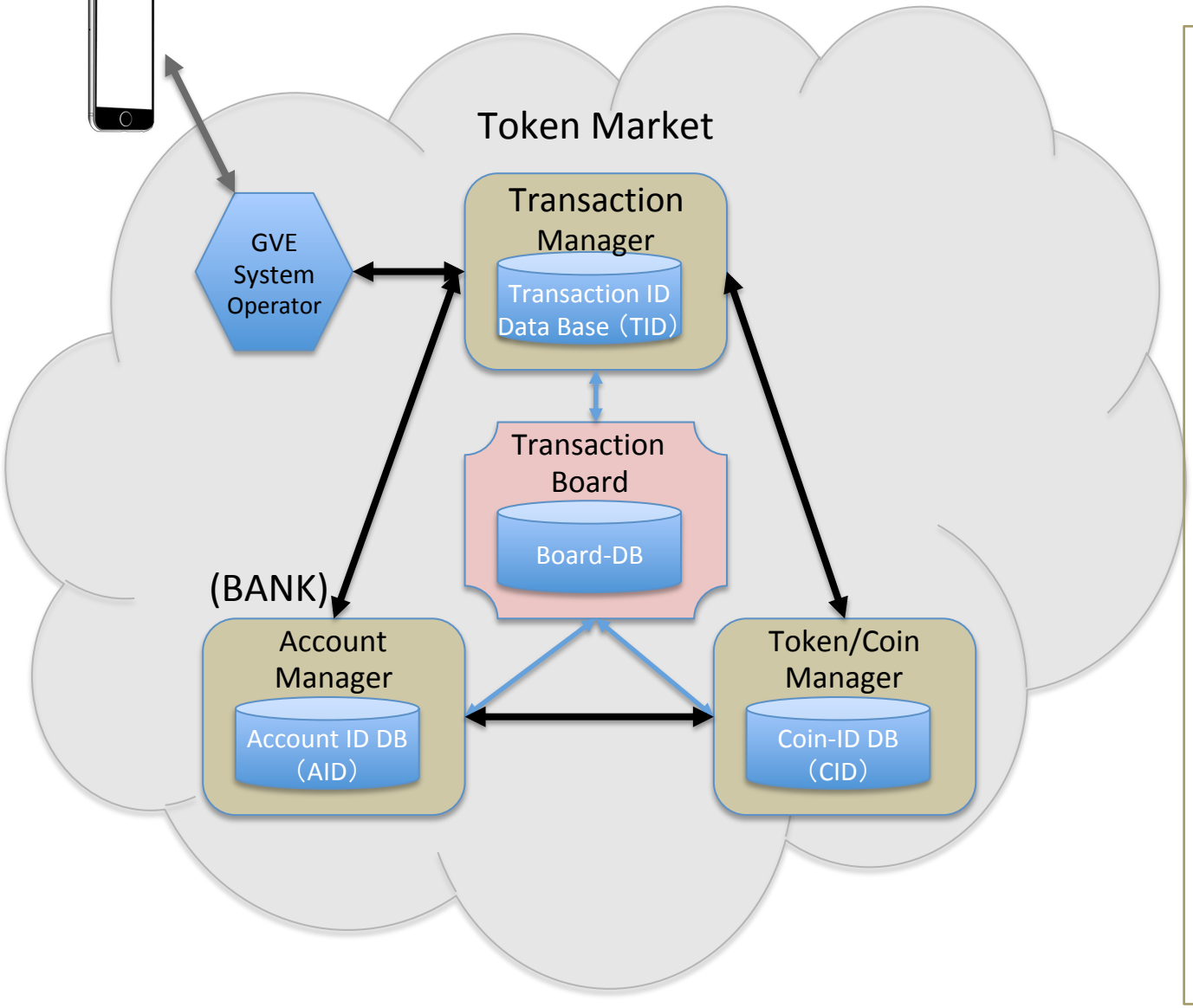
Details of ISO/IEC15408 can be found in the link below

- http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Standard	Edition	Title	Committee
ISO/IEC 15408-1:2009	3rd	nformation technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model	JTC1/SC27
ISO/IEC 15408-2:2008	3rd	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components	JTC1/SC27
ISO/IEC 15408-3:2008	3rd	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components	JTC1/SC27

Smartphone or PC
as client interface of system

EXC Cashless Eco-System



1. Transaction Manager keeps a record of all transactions chronologically.
2. Account Manager and Coin Manager record the same transactions in their respective databases in a different way.
3. Three databases keep the same data in a different way. In this way, each database is able to check the two other databases.
4. There will be a digital signature to confirm the authenticity of transaction
5. The current balance of Account ID DB would be checked by historical transactions
6. These enable the traceability of transactions by the system
7. Transactions not in sync with the terms of conditions, e.g., illegal transactions, could be reversed
8. When HSM is developed, all transactions take place with digital signature incorporating authenticity function
9. We aim to have each transaction settled within 0.2 second when the system development is complete
10. By coordinating with governmental authorities, it would be possible to spot suspected money laundering or other illegal activities