General Security Considerations for Crypto Assets Custodians

draft-vcgtf-crypto-assets-security-considerations

Masashi Sato, Masaki Shimaoka, Hirotaka Nakajima

Background

- We had many security incidents which cause loss of assets.
  - Asia is a “hot” area which suffered from cryptocurrency incidents.

CYBER RISK JANUARY 29, 2018 / 9:36 AM / 9 MONTHS AGO

Japan raps Coincheck, orders broader checks after $530 million cryptocurrency theft

Taiga Uranaka, Thomas Wilson 6 MIN READ

List of major cryptocurrency exchange incidents

Date	Victim	Value of coin loss
Feb 2014	Mt.GOX (Japan)	$450 Million
Aug 2016	Bitfinex (HongKong)	$77 Million
Apr 2017	Youbit (Korea)	$35 Million
Jan 2018	CoinCheck (Japan)	$535 Million
Feb 2018	BitGrail (Italy)	$170 Million
Jun 2018	Coinrail (Korea)	$40 Million
Sep 2018	Zaif (Japan)	$59 Million

Motivations

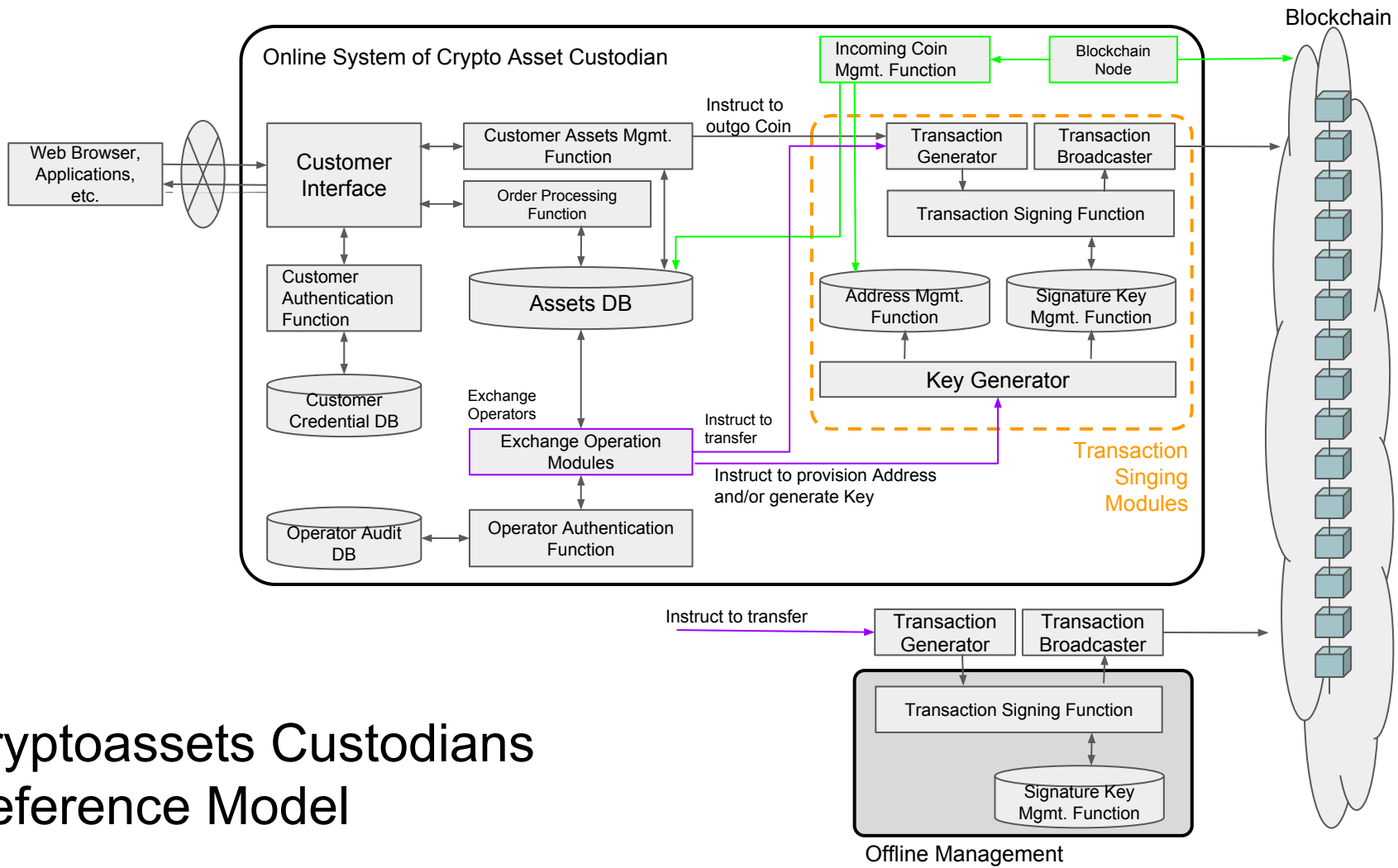
- Build a base document for Crypto Assets custodian’s security (best) practices.
  - No open documents at this moment.
- Share lessons from past incidents without violating a confidentiality obligations (e.g. criminal investigation)

- We are not making a regulations, practices and guidelines.
- Document should be open and globally applicable. (Economics, Regulatory domain free)

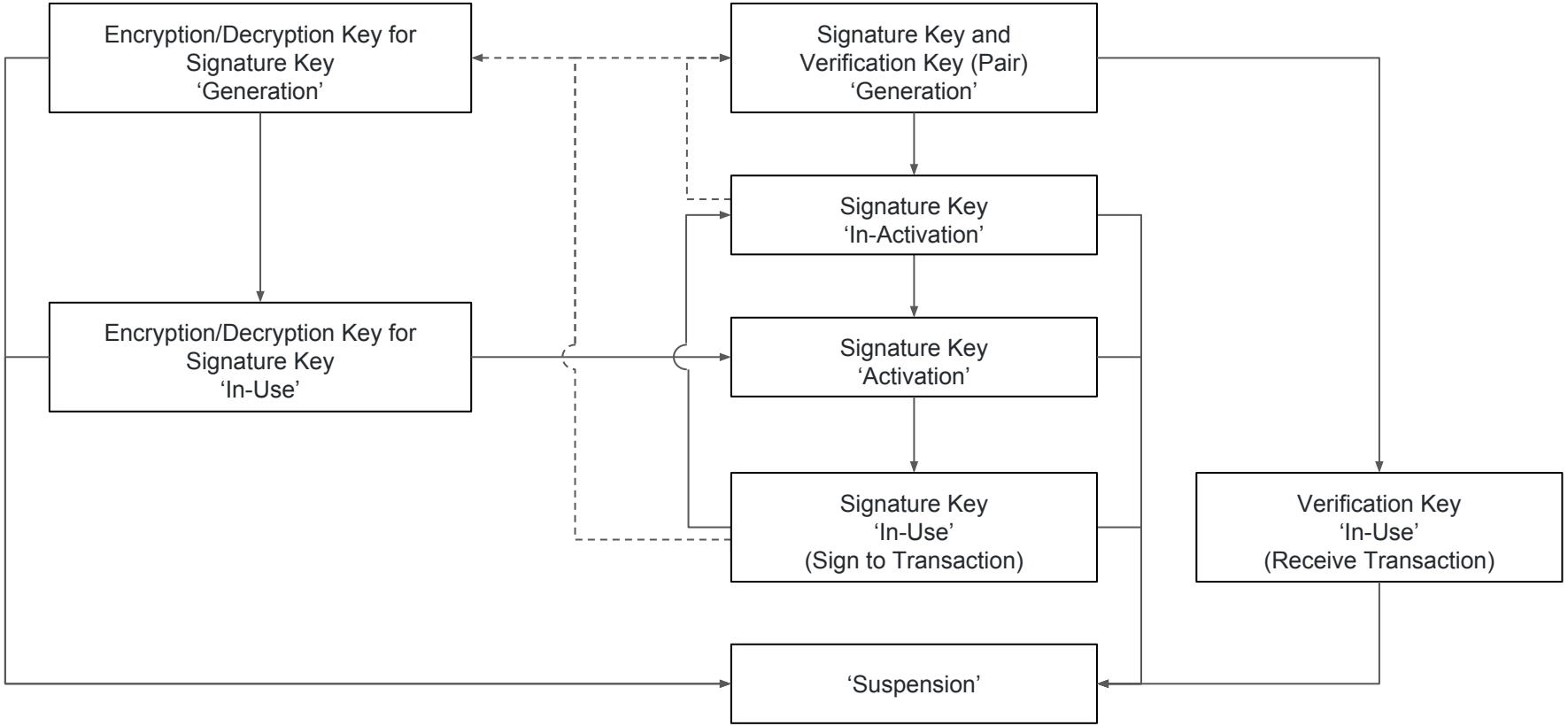
Current Document Structure

- Online systems of crypto assets custodian
  - Reference system model including functional components.
  - Transaction Flow
  - Taxonomy of key management
  - Characteristics of blockchain and distributed ledgers
- Objectives for security management
- Security controls
- Risk Analysis (ISO27001-based)
  - System risk
  - External factors
  - Financial Crime risk

Cryptoassets Custodians Reference Model



Key Lifecycle Model of Crypto assets



Discussions

- IETF is a right place to discuss those issues?
  - If yes, which area/wg is a right place?
    - Sec Area? Or DINRG?
    - Looking for more input (especially from cryptoassets exchanges)
  - If not, are there any alternative places?
    - ISO could be a candidate. But access to draft documents are restricted during the standardization process. (We can’t use the draft document)
- Anti-Money Laundering / Counter Financing of Terrorism
  - Completely out of scope of IETF, but looking a feedback and place where we could get an input.