TAURUS

Protecting Digital Assets: Much More Than Crypto

Jean-Philippe Aumasson, Taurus

March 10th, 2021

Background

Co-founder & chief security officer of **Taurus**

- Geneva-based firm providing digital asset infrastructure
- 2018 foundation, series A funded, team of 25 all in CH
- Market leader among Swiss financial institutions

https://taurusgroup.ch

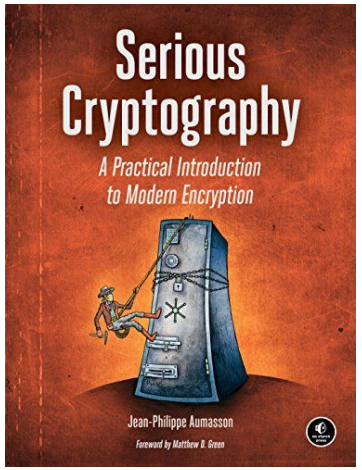
TAURUS PROTECT

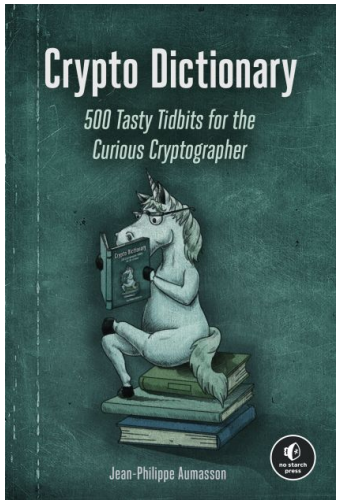
Hot & cold digital assets custody solution

Expert in **cryptography and security**

- Designer of cryptography standards
- Blockchain security auditor
- Author of reference books

https://aumasson.jp





Agenda

1. **Introduction**
2. **Business needs** – Security, compliance, and more
3. **Solutions** – Engineering and shared responsibilities
4. **Secure hardware** – Is it really indispensable?
5. **Conclusion**

Disclaimer

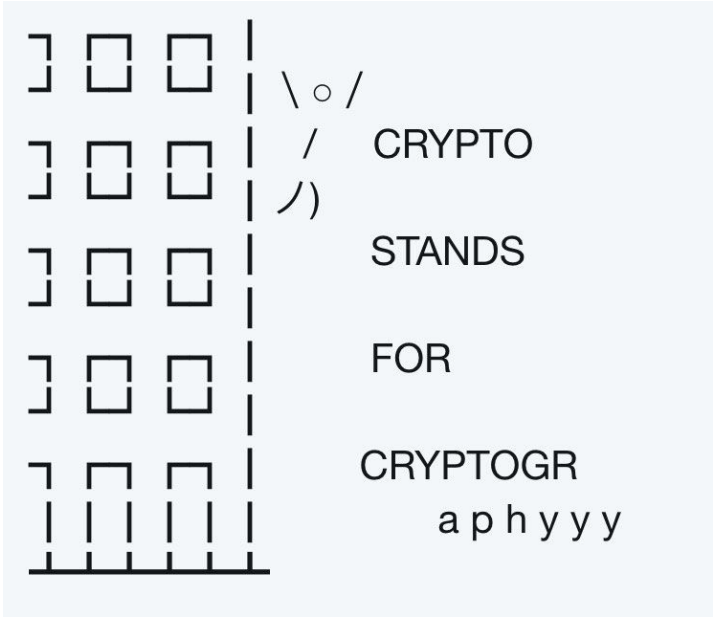
These are my views, not necessarily those of Taurus as a whole

What we describe does not necessarily reflect Taurus' products

Having limited time, this is not a comprehensive overview

Your mileage may vary, this is my own perspective

1. Introduction



Protecting Digital Assets: Much More Than Crypto

A.k.a. crypto assets:

Cryptocurrencies
Digital currencies
Tokenized securities

Protecting Digital Assets: Much More Than Crypto

Theft from insiders and outsiders
Loss of access to the funds
Visibility and privacy issues (CID, etc.)

Generally, alignment with internal risk posture

A.k.a. crypto assets:

Cryptocurrencies
Digital currencies
Tokenized securities

Protecting Digital Assets: Much More Than Crypto

Theft from insiders and outsiders
Loss of access to the funds
Visibility and privacy issues (CID, etc.)

Generally, alignment with internal risk posture

A.k.a. crypto assets:

Cryptocurrencies
Digital currencies
Tokenized securities

Protecting Digital Assets: Much More Than Crypto

Encryption
Signature
Secret-sharing
Pseudorandomness
Multi-party computation

Arsenal of techniques and protocols

Theft from insiders and outsiders
Loss of access to the funds
Visibility and privacy issues (CID, etc.)

Generally, alignment with internal risk posture

A.k.a. crypto assets:

Cryptocurrencies
Digital currencies
Tokenized securities

Protecting Digital Assets: Much More Than Crypto

Software security assurance
Back-up management
Log integrity
etc.

Let's try to understand the needs to address...

Encryption
Signature
Secret-sharing
Pseudorandomness
Multi-party computation

Arsenal of techniques and protocols

2. Business needs

Use cases

Typically several of these:

- **Custody** of crypto assets
- **Transfer** of crypto assets
- **Connectivity to exchanges**' wallets and markets
- Issuance and management of **tokenized securities**
- Creation of **crypto-backed structured products**

Different organizations often have slightly different needs:

Investment banks	Cantonal, retail, digital banks	Private banks	Crypto-banks	Financial infrastr. providers

Integration needs

Banks requires functionalities and security controls permitting regulatory compliance, and compatible with internal IT and risk management processes

Example of such functionalities and controls encountered:

COMPLIANCE

- FINMA 3 lines of defense
- Off-balance sheet accounting

GOVERNANCE

- Role-based access
- Per-wallet rules

RISK MANAGEMENT

- Address whitelisting
- Operations rate-limiting

WALLET MANAGEMENT

- Segregation of wallets
- Large number of addresses

TRANSACTION MANAGEMENT

- Fee management
- Transaction audit trail

ANALYTICS

- Fast reconciliation
- KPI generation

Security goals – Specific examples

Prevent direct access to the seeds or keys

Prevent unauthorized access to signing capabilities

Prevent unauthorized transactions creation

Generate and back-up keys securely

Protect logs and databases information

Ensure supply chain and software build integrity

Security goals – General

The system should be auditable. It must provide records to the security control supervisor, so that system performance, security safeguards and user activities can be monitored. This implied that both manual and automatic monitoring facilities were desirable.

The system should be reliable from a security point of view. It ought to be fail safe in the sense that if the system cannot fulfill its security controls it will withhold information from those users about which it is uncertain, but ideally will continue to provide service to verified users. A fallback and independent set of security safeguards must be available to function and to provide the best level of security possible under the degraded conditions if the system is to continue operation.

The system should be manageable from the point of view of security control. The system should be supplemented by the capability to make appropriate modifications in the operational status of the system in the event of catastrophic system failure, degradation of performance, change in workload or conditions of crisis.

In NSA's 1998 *History of Computer Security*
https://cryptome.org/2020/10/nsa-history-computer-security-1998.pdf

Security goals – General

Examples:

The system should be auditable. It must provide records to the security control supervisor, so that system performance, security safeguards and user activities can be monitored. This implied that both manual and automatic monitoring facilities were desirable.

Transparency, audit trails

The system should be reliable from a security point of view. It ought to be fail safe in the sense that if the system cannot fulfill its security controls it will withhold information from those users about which it is uncertain, but ideally will continue to provide service to verified users. A fallback and independent set of security safeguards must be available to function and to provide the best level of security possible under the degraded conditions if the system is to continue operation.

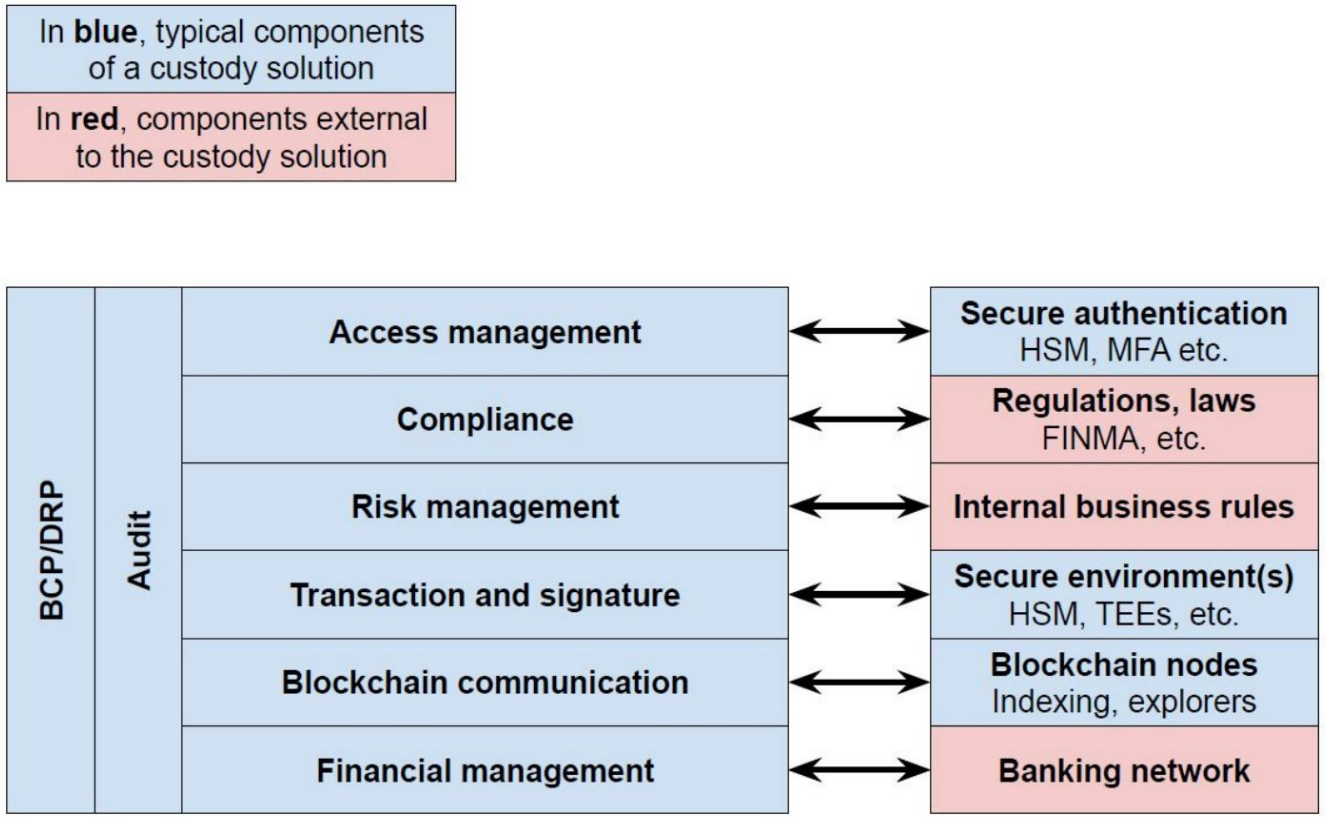
Failover systems, safe error handling and reporting

The system should be manageable from the point of view of security control. The system should be supplemented by the capability to make appropriate modifications in the operational status of the system in the event of catastrophic system failure, degradation of performance, change in workload or conditions of crisis.

Customisable and redundant security controls to mitigate failure of other systems

In NSA's 1998 *History of Computer Security*
https://cryptome.org/2020/10/nsa-history-computer-security-1998.pdf

Custody security model

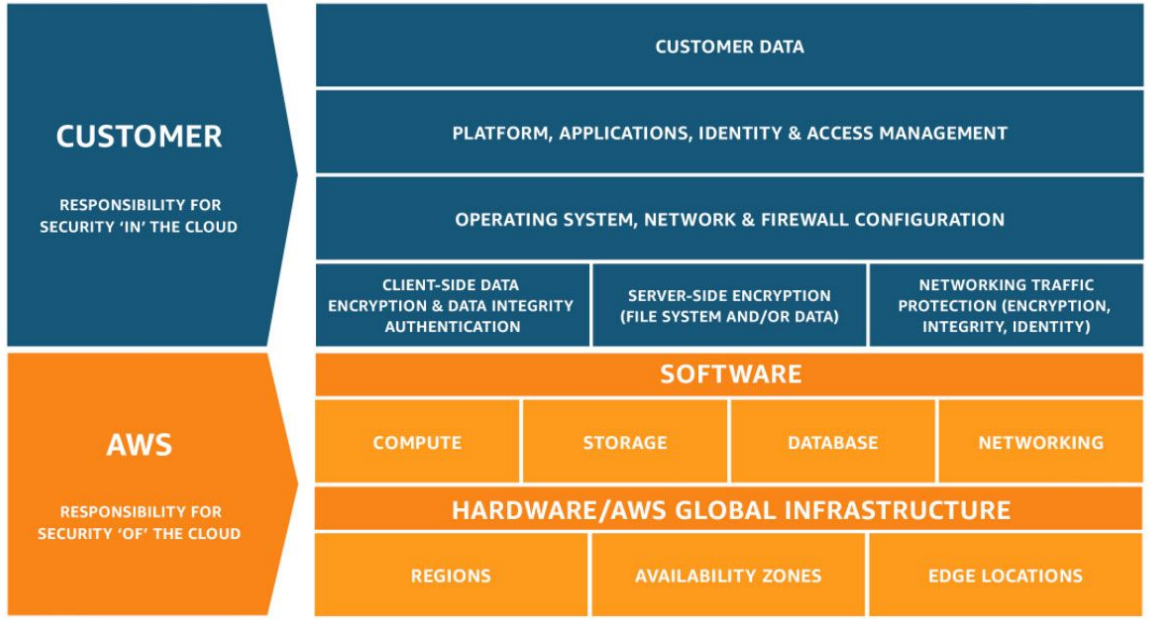


In Taurus' *Views on banking-grade digital asset custody solutions*
https://www.taurusgroup.ch/articles/20201027_Banking_Grade_Custodian/20201027%20Taurus_Banking_Grade_Custody_final.pdf

3. Solutions

Shared responsibilities

Security and compliance is a shared responsibility between the solution provider and the client organization, as described by AWS for cloud services:



Shared responsibility model for AWS cloud services
https://aws.amazon.com/compliance/shared-responsibility-model/

Custody solution, on-premise or cloud, also involve shared responsibilities...

Security controls and shared responsibilities

Example controls from our security model: provider, client, both
(The responsibility distribution might depend on the operating model)

Access management

- Effective role-based access mechanism
- Secure configuration and assignment or roles

Compliance

- Effective subsystems supporting KYC and AML compliance
- Proper usage & configuration thereof, compliant operation

Transaction and signature

- Secure storage and processing of keys, quorum validation mechanism
- Secure and correct key derivation and transaction creation

Security controls and shared responsibilities

Example controls from our security model: provider, client, both
(The responsibility distribution might depend on the operating model)

Blockchain connectivity

- Reliable broadcasting of transactions
- Non-transmission of sensitive/personal information

Risk management

- Whitelisting/blacklisting, rate-limiting, authorized time rules
- Proper configuration of rules and distribution of admin roles

Business continuity & Disaster recovery

- High-availability managed services
- Redundant backups and recovery procedures

The key ceremony case

Critical procedure that is about much more than using a reliable pseudorandom generator, involving notably procedures to ensure:

- **Auditability** of procedure, scripts, software components, ceremony operations
- Practical impossibility of software or hardware **sabotage**
- **Recoverability** of secrets under any circumstance for the foreseeable future

The key ceremony case

Critical procedure that is about much more than using a reliable pseudorandom generator, involving notably procedures to ensure:

- **Auditability** of procedure, scripts, software components, ceremony operations
- Practical impossibility of software or hardware **sabotage**
- **Recoverability** of secrets under any circumstance for the foreseeable future

Example technologies and procedures involved in Taurus' ceremonies:

- **Cryptographic** secret-sharing and signature mechanisms
- **Verified build** of critical software overseen by an external security auditor
- Formal **request-review-approval** process for any change in the documentation

4. Secure hardware

Hardware security modules (HSMs)

Pieces of hardware dedicated to security functionalities

Typically, **storing secret keys** and doing associate processing

Often covered by certifications concerned with tamper detection and resistance

Hardware-less approaches?

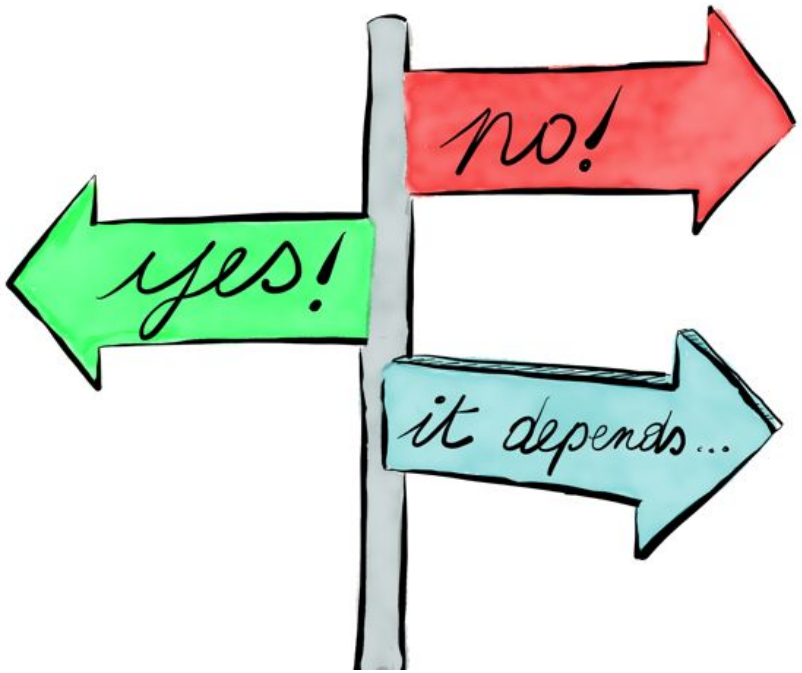
Multi-party computation (MPC) leverages cryptographic protocols to distribute private keys over multiple systems (pure software, or with hardware-level security)

“Can **MPC** be sufficient for a software-only custody platform?”

Hardware-less approaches?

Multi-party computation (MPC) leverages cryptographic protocols to distribute private keys over multiple systems (pure software, or with hardware-level security)

“Can **MPC** be sufficient for a software-only custody platform?”



- **Operating model**: asset shared control vs. SaaS custody vs. self-custody
- **Security assurance** requirements
- **Functional** requirements
- **Segregation** capabilities

HSM and MPC offer different functionalities

HSM

- Signature without exposing the key, in an isolated environment
- Trusted execution of business logic, such as security controls and rules
- Physical attacks mitigation, with certified equipment (e.g. FIPS 140-2)
- Role-based access for configuration, access, privilege levels

MPC

- Secure signature without exposing the key, via a cryptography protocol

MPC operational aspects:

- Key shares distributed on multiple segregated systems (software or hardware)
- Enables software-only signature with a reasonable assurance level
- Potentially lower acquisition cost and higher scalability
- Needs reliable network connectivity between multiple sites

5. Conclusions

Takeaways

Banking-grade custody is very different from personal wallets

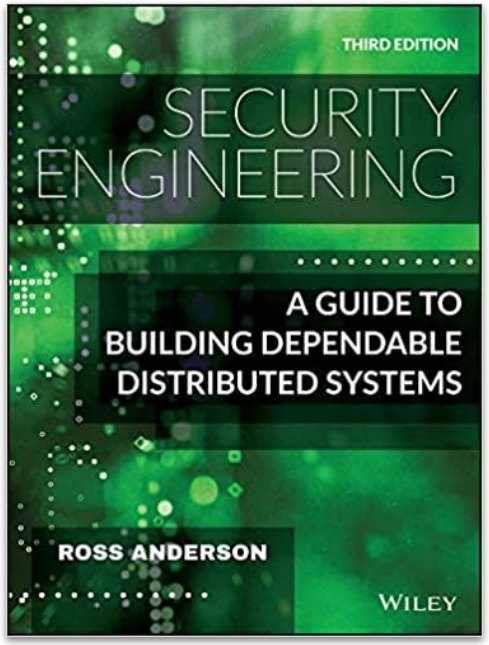
The security principles apply more than ever:

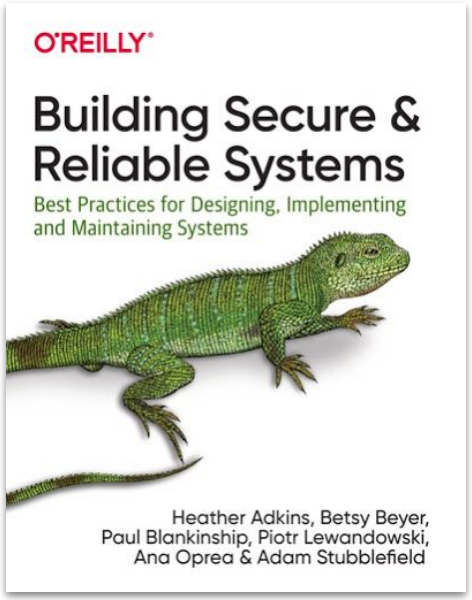
- Security is a process, not a state
- Security is about people, processes, and technology

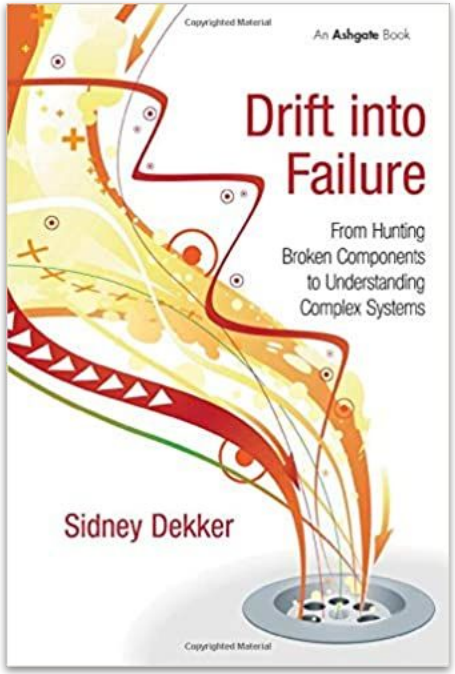
Different use cases call for different approaches (hot/cold, SaaS/on-premise)

Hardware-level security is mandatory to mitigate certain risks, but such risks may be acceptable depending on the use case

Recommended reading







https://www.taurusgroup.ch/en/insights/taurus-banking-grade-digital-assets-custodian

Thank you!
Danke!
Merci!
Grazie!

https://taurusgroup.ch, where these slides will be published

jp@taurusgroup.ch, please don't hesitate to contact me

https://twitter.com/veorq, for personal ramblings about cryptography :)