Key Management Tasks

SIGS Event February 9th, 2017

About & Beyond PKI

marcel.suter@libC.ch

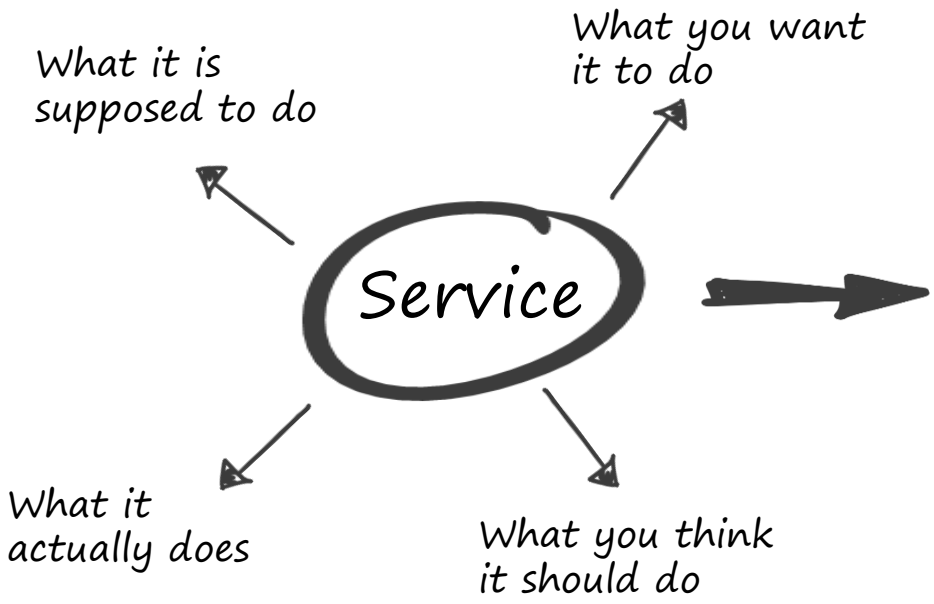
libC Technologies Sàrl
Case postale 57
1804 Corsier-sur-Vevey

www.libC.ch
info@libc.ch
T: +41 21 550 1562

Agenda

- Security Services
- Key Management
  - Planning
  - Specifications
- Use Cases
  - Out of the box PKI
  - Standard PKI deployments involving HSMs
  - PKI deployments involving HSMs and Smartcards
- Key Generation
- Keys in the Cloud
- Conclusion
- Q&A

Security Services



Security?

- Confidentiality
- Data Integrity
- Integrity authentication
- Source authentication
- Authorization
- Non-repudiation
- Support services (RNG)
- Combined services

libC Technologies Sàrl
Case postale 57
1804 Corsier-sur-Vevey

www.libC.ch
info@libc.ch
T: +41 21 550 1562

Key Management

libC TECHNOLOGIES

Planning

- Security Services
- Cryptographic Algorithms
- Key Types
- Key Usages (one usage == one key)
- Cryptoperiods
- Assurances
- Key Compromise
- Key Sizes
- Protection Requirements
- Protection Mechanisms
- Key States/Transitions
- Key Management Phases
- Accountability, Audit
- Contingency

Specification

- Aspects of the Cryptographic Application
- Communication Environment
- Key Management
- Key Generation
- Key Distribution
- Key Storage
- Access Control
- Key Material Accounting
- Key Recovery
- Key Compromise

libC Technologies Sàrl
Case postale 57
1804 Corsier-sur-Vevey

www.libC.ch
info@libc.ch
T: +41 21 550 1562

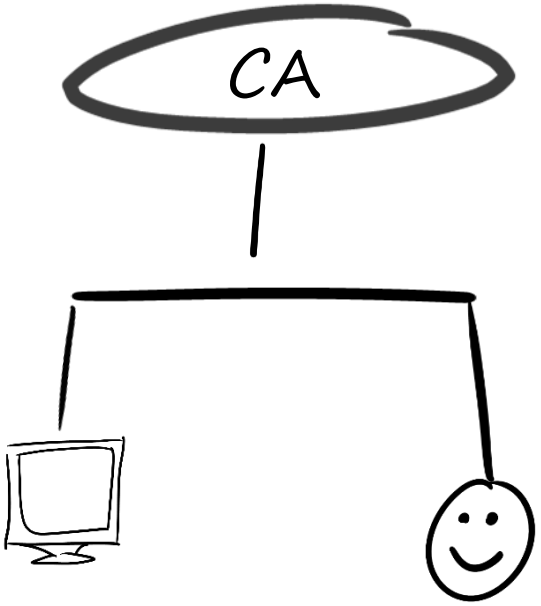
An illusion of security

libC Technologies Sàrl
Case postale 57
1804 Corsier-sur-Vevey

www.libC.ch
info@libc.ch
T: +41 21 550 1562

libC TECHNOLOGIES

- ☑ Mechanisms
- ☒ Protocols
- ☒ Afforded key protection
- ☒ Protection against key modification
- ☒ Protection against unauthorized disclosure
- ☒ Secure key generation
- ☒ Secure key storage
- ☒ Secure key distribution
- ☒ Secure key usage
- ☒ Secure key destruction



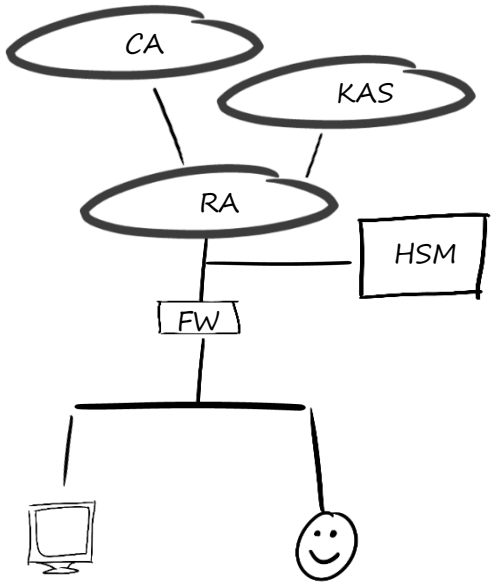
libC Technologies Sàrl
Case postale 57
1804 Corsier-sur-Vevey

www.libC.ch
info@libc.ch
T: +41 21 550 1562

Standard PKI

Hardware Keys for PKI and Software Keys for End Users/Systems

HW	SW	
☑	☑	Mechanisms
☑	☒	Protocols
☑	☒	Afforded key protection
☑	☒	Protection against key modification
☑	☒	Protection against unauthorized disclosure
☒	☒	Secure key generation
☑	☒	Secure key storage
☑	☒	Secure key distribution
☑	☒	Secure key usage
☑	☒	Secure key destruction



libC Technologies Sàrl
Case postale 57
1804 Corsier-sur-Vevey

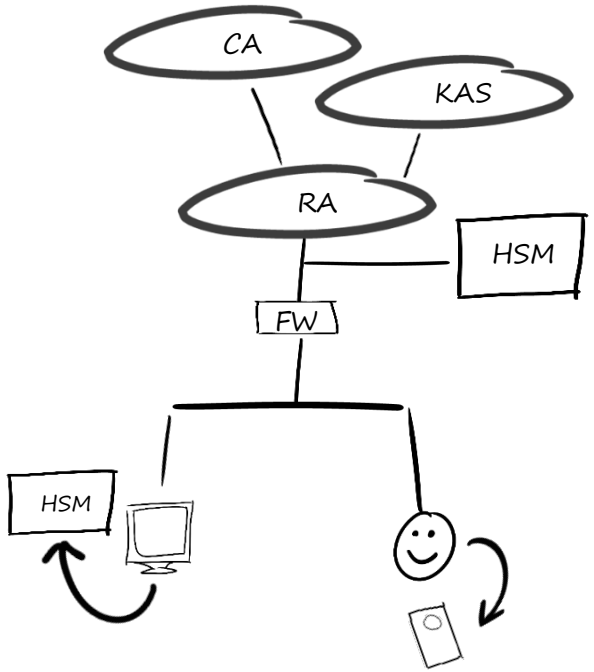
www.libC.ch
info@libc.ch
T: +41 21 550 1562

PKI with Smartcards

Hardware Keys for PKI and End Users/Systems

libC TECHNOLOGIES

- ☑ Mechanisms
- ☒ Protocols (network vs USB)
- ☑ Afforded key protection
- ☑ Protection against key modification
- ☑ Protection against unauthorized disclosure
- ☒ Secure key generation
- ☑ Secure key storage
- ☒ Secure key distribution (key recovery)
- ☑ Secure key usage
- ☑ Secure key destruction



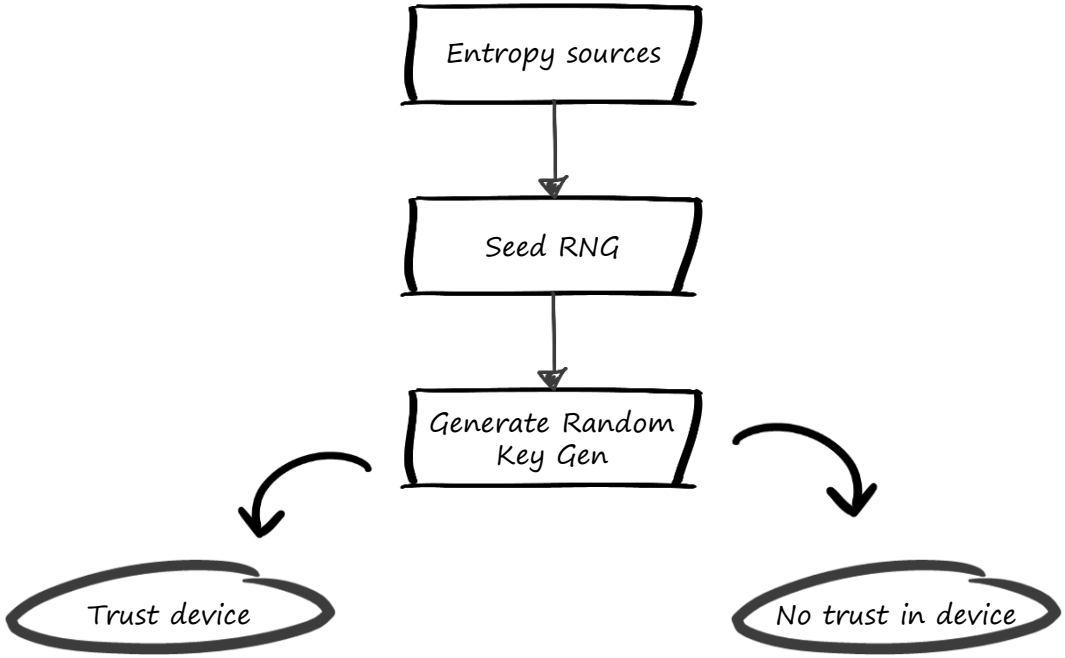
libC Technologies Sàrl
Case postale 57
1804 Corsier-sur-Vevey

www.libC.ch
info@libc.ch
T: +41 21 550 1562

Key Generation

To trust or not to trust

libC TECHNOLOGIES



- Validate entropy sources
- Verify manufacturer's Seed RNG implementation
- Verify manufacturer's Generate Random implementation
- Verify manufacturer's Key Generation implementation

- Manufacturer dependency
- Key extraction usually impossible from HW device

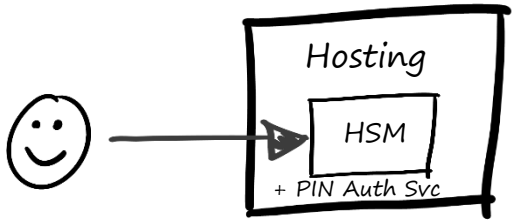
- SW key generation procedure
  - Control over entropy sources
  - Control over RNG Seed
  - Control over Generate Random and Key Generation
- SW key injection into device
- Disposal and wipeout of SW key generation device
- Generated SW key secure archiving
- No manufacturer dependency

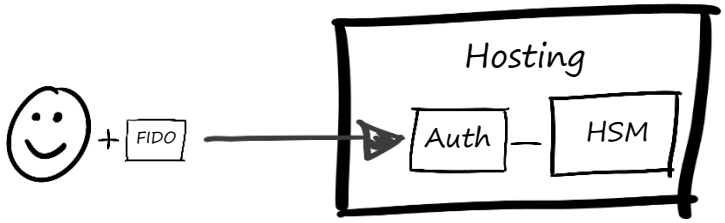
libC Technologies Sàrl
Case postale 57
1804 Corsier-sur-Vevey

www.libC.ch
info@libc.ch
T: +41 21 550 1562

Keys in the Cloud

libC TECHNOLOGIES





- Solves your renewal, recovery, dependency on smart cards, key protection, key modification, key distribution, key usage, key destruction
- Secured client/partition communication implemented via ECDH, AES-GCM
- Customer master keys represent the top level key hierarchy. Everything underneath it is ciphered with this master key

- Choose hosting with care, think twice: 5th + EU
- You loose 2FA
- Partition PIN access provides insufficient protection
- Cloud services offer FIPS 140-2 Level 2 (Azure), not yet FIPS validated for Amazon
- No control over RNG
- Proprietary authentication mechanism
- DDOS

- Solves your renewal, recovery, dependency on smart cards, key protection, key modification, key distribution, key usage, key destruction
- Secured client/partition communication implemented via ECDH, AES-GCM
- FIDO token provides the integrity and the second factor (+PIN)
- Uses a second PIN to access the master encryption key

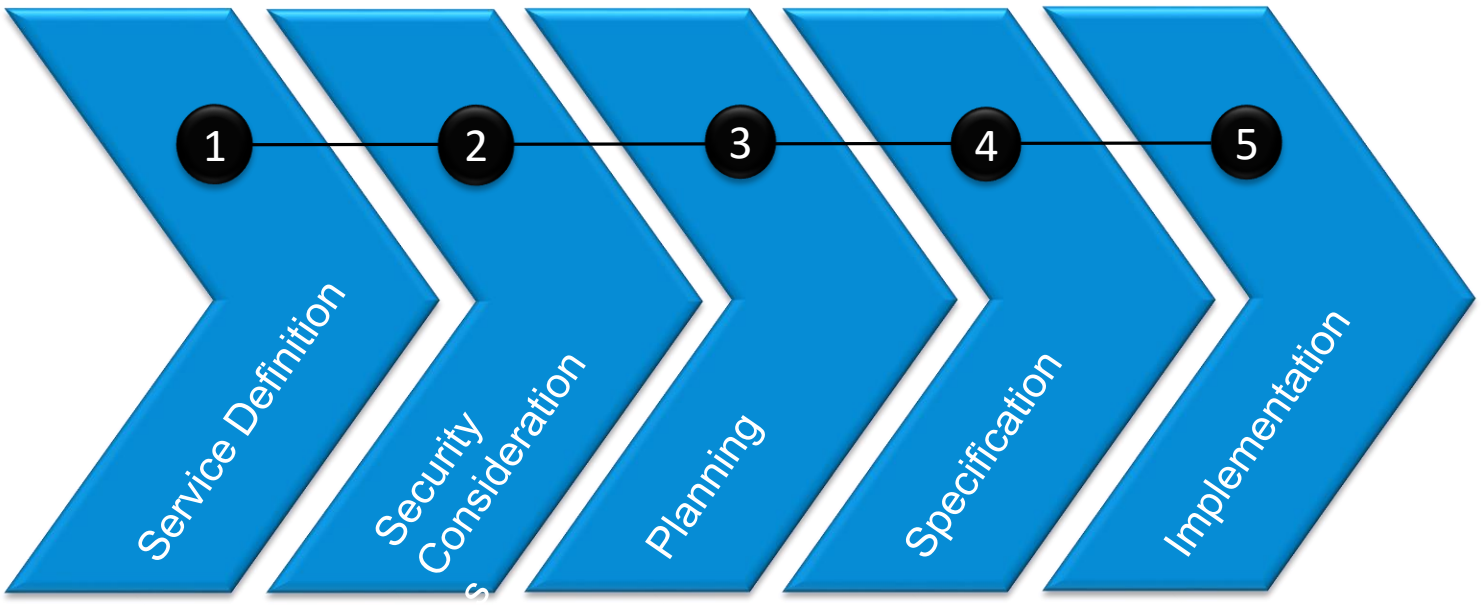
- Choose hosting with care, think twice: 5th + EU
- No control over RNG
- DDOS

libC Technologies Sàrl
Case Postale 57
1804 Corsier-sur-Vevey

www.libC.ch
info@libc.ch
T: +41 21 550 1562

Conclusion

libC TECHNOLOGIES



libC Technologies Sàrl
Case postale 57
1804 Corsier-sur-Vevey

www.libC.ch
info@libc.ch
T: +41 21 550 1562