

Streamlining Key Management

An Innovative and Audit-Friendly Approach



Rolf Pielage

Senior Manager Cyber Security @ Deloitte Netherlands
Cyber, Cryptography, Payments/IoT/ICS

Deloitte.



Kris Olejniczak

CEO, Patronusec
PCI QSA, P2PE QSA, SSF QSA, QPA, 3DS QSA



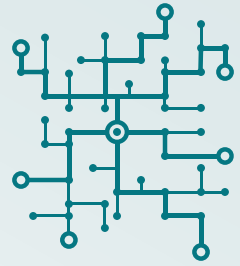
PATRONUSEC
Your Cyber Security Patronus



Industry insights



Common approach to Key Management



Complex process - hard to automate



Expensive - time and resources consuming



Hard to audit and trace



Equally - important for payments security

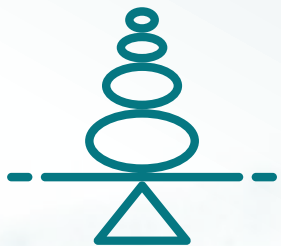
Reasons for manual key management



Not main interest of personnel



Difficult



“It was always like that”



Limited access to technology and documentation

What if ?



Re-think key management



Traceable process



No manual paperwork



Remove human error element



Efficient system

Automation



How we achieved automation ?

1

Repeatable process

2

Central server to manage all key generation

3

Offline client software in the Secure Room

4

Repository for affidavits and reports

5

PCI compliant way

A hand holding a magnifying glass over a network diagram. The word "Details" is centered in the lens of the magnifying glass. The background is a light blue network of nodes and lines, with some nodes highlighted in orange.

Details

Architecture

Online components

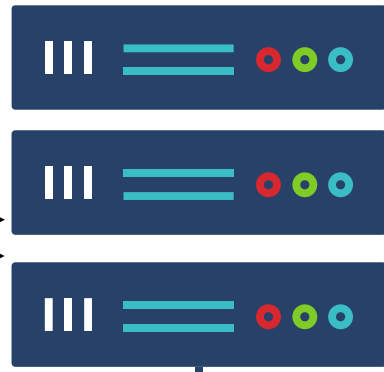
Offline

Client / auditor



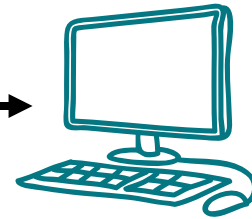
Read-only access

DKMT



API

Script Generation Tool



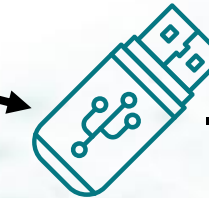
Paper script



Digital input file



Load



Load



Communication

Print components



HSM

Output file



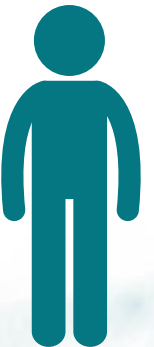
Sign



Key Ceremony Attendants



Manage sealbags & shipments



Key Guardian

Upload signed paper affidavits



Key Management Administrator

Import results



Offline key management tool



Implementation details

Example affidavit

Table of Contents

1. Affidavit for Key Management Session.....	1
1.1. Deloitte KMS Operation Security Process Protocol.....	1
1.2. Security Process Steps.....	1
1.3. Signatures.....	2
1.4. Additional session notes.....	2
1.5. Emergency procedures.....	3
2. Guardian preparations.....	4
2.1. Required seal bags to execute script.....	4
3. Session Script.....	
3.1. Open secure rack.....	
3.2. Start Computer.....	
3.3. Check DKMT_AES_KB.....	
3.4. Load DKMT_AES_KB (152).....	
3.5. Generate and Export DKMT_AES_KB (152).....	
3.6. Close DKMT_AES_KB (152).....	
3.7. Stop Computer.....	
3.8. Session Closure.....	
3.9. Close secure rack.....	

1.4. Additional session notes

Produced using Key Script tool, version 4.2.2

Table 3. Required seal bags

	Seal bag ID	Description	Date	Guardian	Location
<input type="checkbox"/>	12345	DKMT Test Laptop	2018-05-16	Deloitte	ZA0
<input type="checkbox"/>	12360	LMK_TEST_AES COMP 3 COPY 1	2018-05-09	GG3	ZA0
<input type="checkbox"/>	12368	LMK_TEST_AES COMP 1 COPY 1	2018-05-09	GG1	ZA0
<input type="checkbox"/>	12369	LMK_TEST_AES COMP 2 COPY 1	2018-05-09	GG2	ZA0

Implementation details

Offline software

The screenshot displays a software interface with two main panels. The left panel contains a list of six steps for HSM configuration, and the right panel shows a dialog box for connecting to a serial interface. Below these panels is a log window.

1) CheckHSM
firmware_name: deloitte_km
hsm: HSM S0123456789N
role: 'Role: deloitte_km, FW: 1234-0000'

2) LoadLMK
hsm: HSM S0123456789N
lmk: LMK_TEST_AES

3) GenerateKeyUnderLMK
hsm: HSM S0123456789N
key: BDK_TEST_1
key_length: '2'
lmk: LMK_TEST_AES

4) GenerateKeyUnderLMK
hsm: HSM S0123456789N
key: CVK_CVV_TEST_1
key_length: '2'
lmk: LMK_TEST_AES

5) GenerateKeyUnderLMK
hsm: HSM S0123456789N
key: IMKAC_TEST_1
key_length: '2'
lmk: LMK_TEST_AES

6) GenerateKeyUnderLMK
hsm: HSM S0123456789N
key: IMKIDNK_TEST_1
key_length: '2'
lmk: LMK_TEST_AES

Connect serial interface to HSM S0123456789N

OK

Cancel

Log

2024-08-27 17:23:55 - Input file checksum is: FD 54 15 75 CA 41 2C 3D 3C 7D 25 61 68 4F B2 A2 9C DE 5D 66 43 28 18 2C 99 6D 68 E1 AE 07 C4 3C
2024-08-27 17:23:57 - Creating output file
2024-08-27 17:23:57 - Running step: CheckHSM: {'hsm': 'HSM S0123456789N', 'role': 'Role: deloitte_km, FW: 1234-0000', 'firmware_name': 'deloitte_km'}
2024-08-27 17:23:58 - Scanning for HSM S0123456789N via serial

Implementation details

Central software overview

Key

Columns ¹ Filters Density

ID	Name	Description ▼	Key type	KCV	Created ↓	Expires	
440	BDK_TEST_2		BDK	15FD35	2022-12-21	1904-12-31	>
441	CVK_CVV_TEST_2		VISA_CVK	58DAC8	2022-12-21	1904-01-01	>
442	PVK_PVV_TEST_2		VISA_PVK	532D5E	2022-12-21	1904-01-01	>
443	ZKA_TEST_2		ZKA	046C04	2022-12-21	1903-01-01	>
444	ZMK_DKMT_AES_KBAUTH_2		ZMK	9B59EC	2022-12-21	1904-12-31	>
445	ZMK_DKMT_AES_KBFF_2		ZMK	420AFB	2022-12-21	1904-12-31	>
446	ZPK_TEST_2		ZPK	00EC4C	2022-12-21	1903-01-01	>
447	ZKA_TEST_TR31_2		ZKA	14C75D	2022-12-21	1903-01-01	>

Implementation details

Central software - edit key screen

Dashboard

Planning

- REQUESTS
- CEREMONIES

Administration

- KEYS
- COMPONENTS
- KEY TYPES
- COMPONENT TYPES
- KEY STATUS
- KEY FILES
- SEAL BAGS
- LOCATIONS
- CUSTODIANS
- GROUPS

Edit Key

Select a key type *	Name *	Check value	
ZMK	TEST_ZMK_10	ABCDEF	
Key status *	Description	Comments	
Loaded	New description	test	
Created	In use since	Custom expiration	Destructed
2023-04-13			

Key type based information

Tag

Takeaways



Automation benefits



Organization

- Little involvement while maintaining control
- Compliance with applicable standards
- No SPOFs as knowledge is in code

WIN



Auditor

- Traceable process
- Cost efficient audit process
- Increased confidence in audit results



Key Manager

- Efficient process
- Central evidence repository
- Chain of custody

How YOU can achieve automation

1

Create a repeatable process

2

Make it simple and eliminate waste

3

Make business case

4

Use automation opportunity

5

Digitalize evidence (blockchain-like technology)

Thank you

For any questions, please contact us



Kris: Kris.Olejniczak@patronusec.com



<https://www.linkedin.com/in/olejniczak>



Rolf: RPielage@deloitte.nl



<https://www.linkedin.com/in/rolfpielage>





Security Standards Council[®]