Streamlining Key Management

An Innovative and Audit-Friendly Approach

PCI Security Standards Council

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

PCI Security Standards Council

Industry insights

PCI Security Standards Council

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

PCI Security Standards Council

Reasons for manual key management

Not main interest of personnel

Difficult

“It was always like that”

Limited access to technology and documentation

What if ?

PCI Security Standards Council

Re-think key management

Traceable process

No manual paperwork

Remove human error element

Efficient system

PCI Security Standards Council

Automation

PCI Security Standards Council

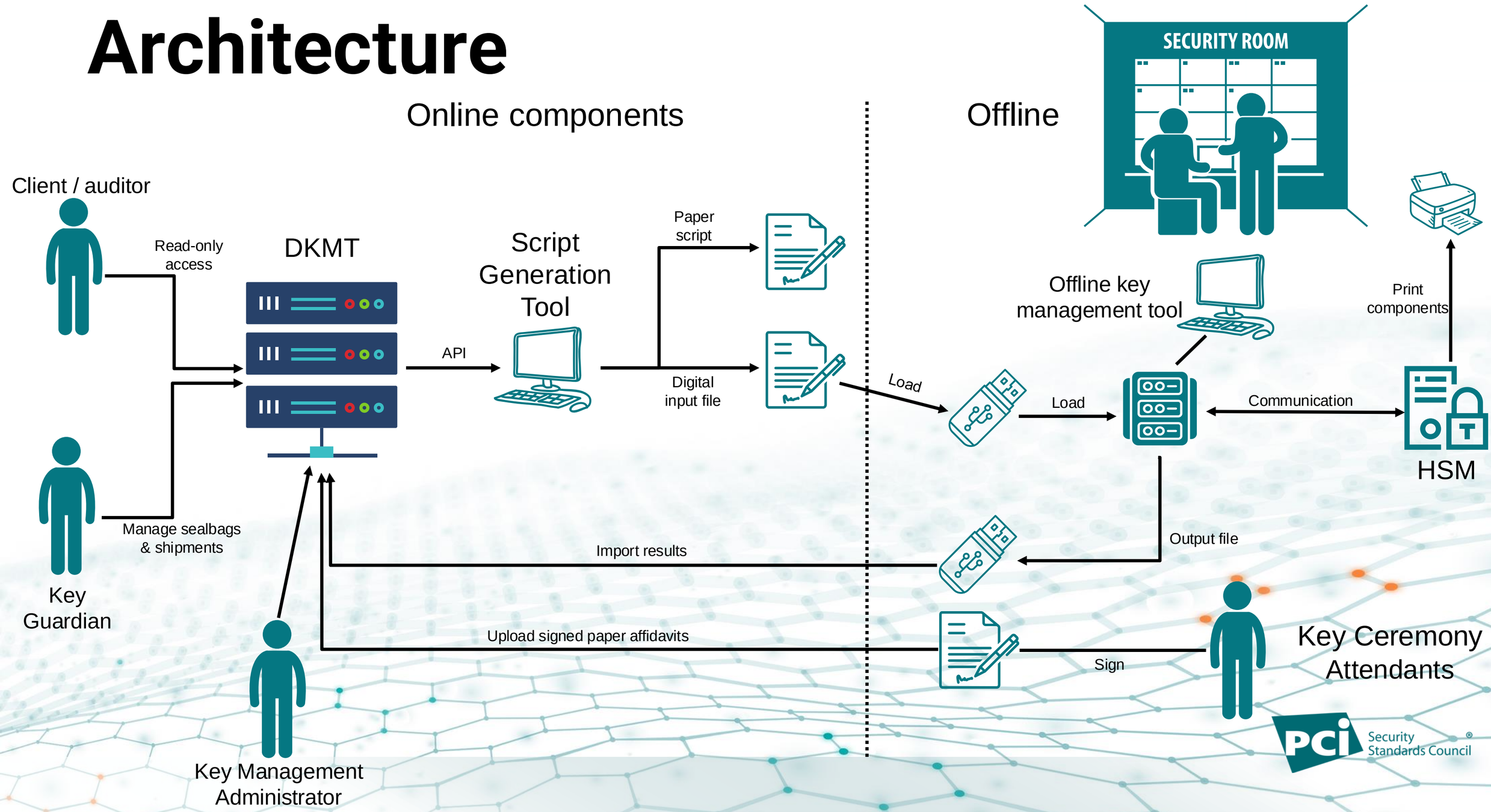
How we achieved automation ?

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

PCI Security Standards Council

PCI Security Standards Council

Architecture



Implementation details

Example affidavit

Table of Contents

1.4. Additional session notes

Produced using Key Script tool, version 4.2.2

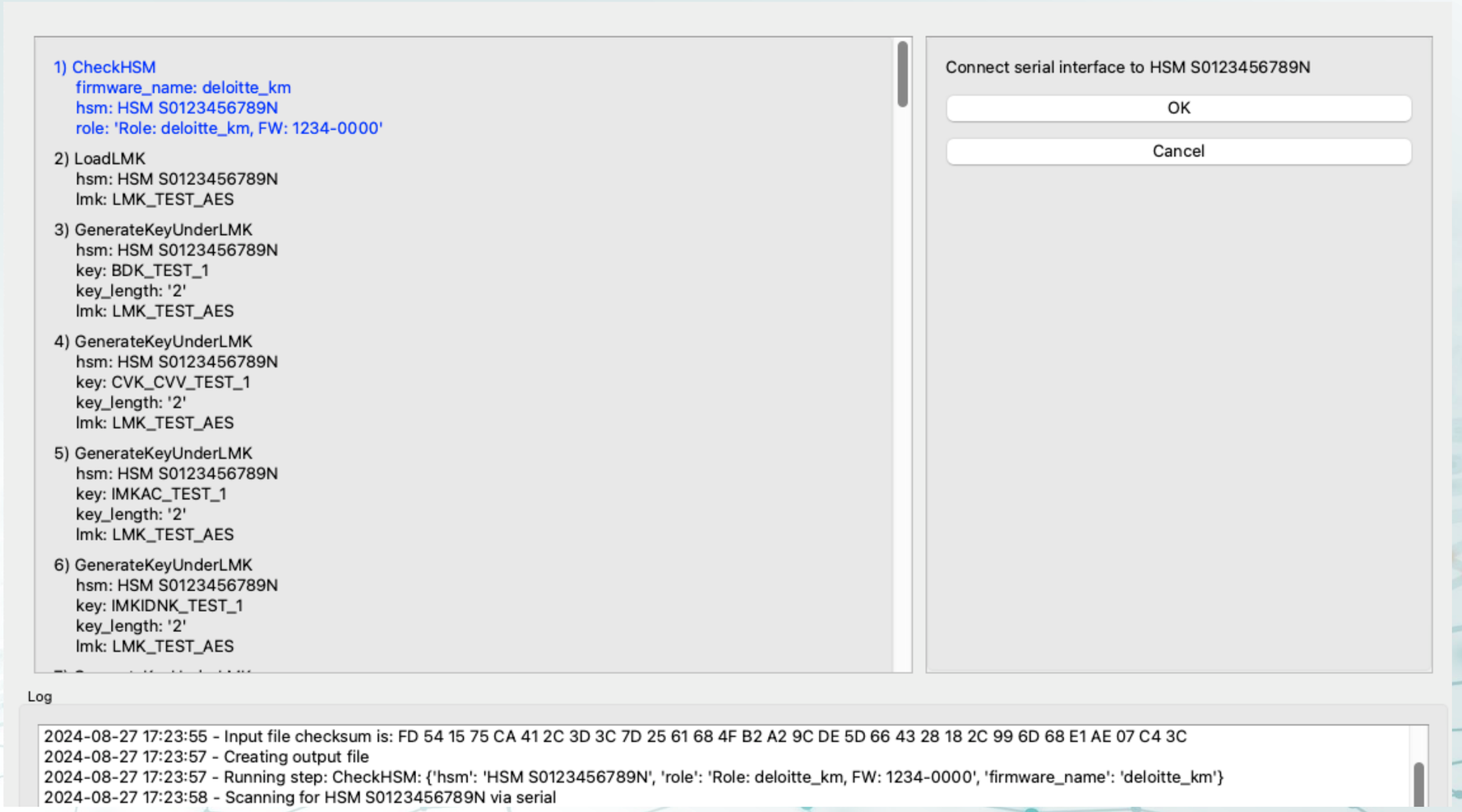
Table 3. Required seal bags

	Seal bag ID	Description	Date	Guardian	Location
☐	12345	DKMT Test Laptop	2018-05-16	Deloitte	ZA0
☐	12360	LMK_TEST_AES COMP 3 COPY 1	2018-05-09	GG3	ZA0
☐	12368	LMK_TEST_AES COMP 1 COPY 1	2018-05-09	GG1	ZA0
☐	12369	LMK_TEST_AES COMP 2 COPY 1	2018-05-09	GG2	ZA0

PCI Security Standards Council

Implementation details

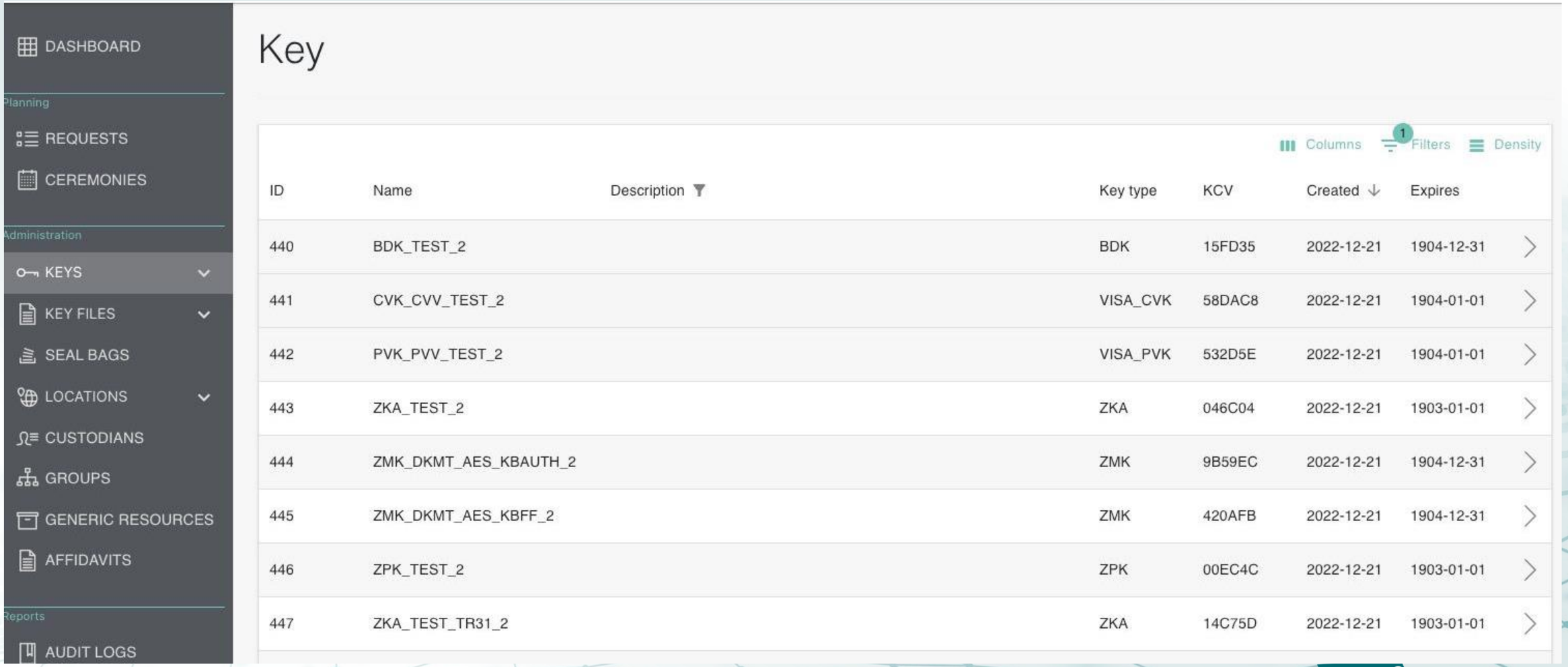
Offline software



PCI Security Standards Council

Implementation details

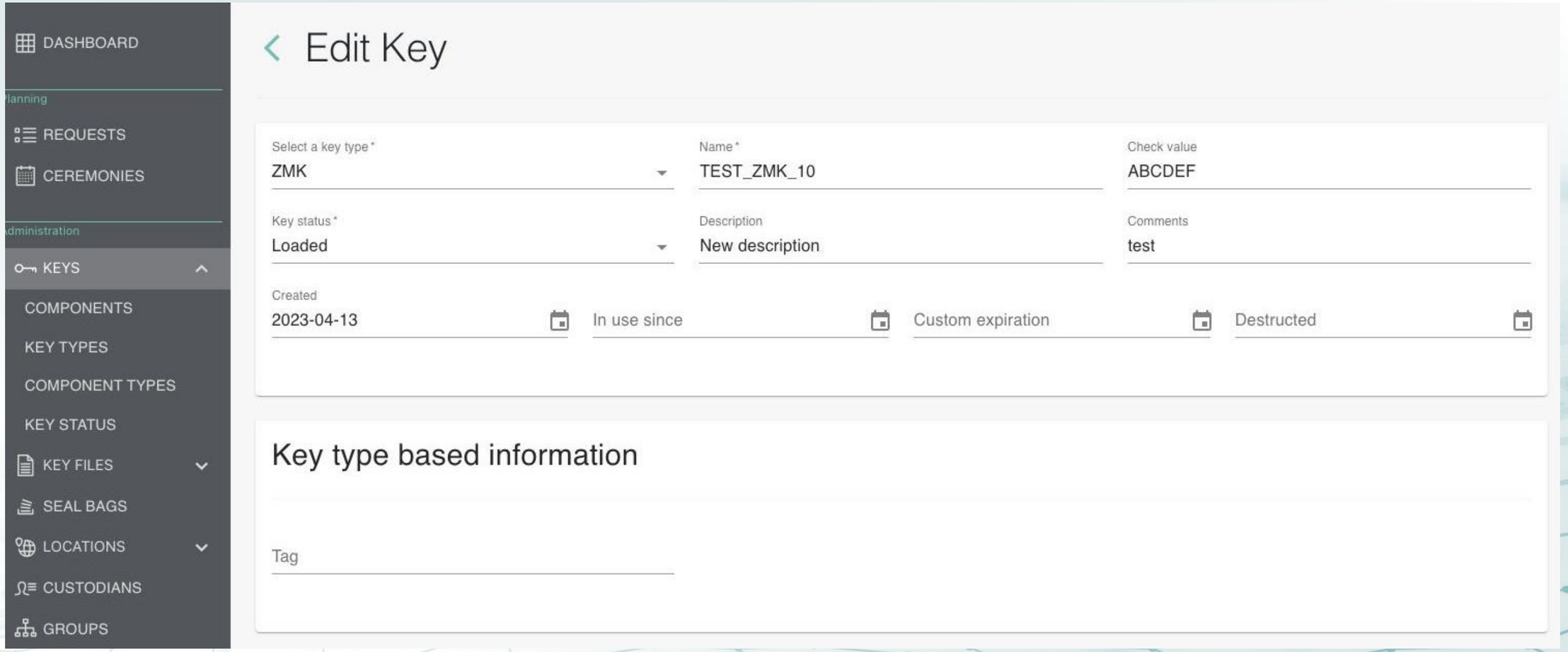
Central software overview



PCI Security Standards Council

Implementation details

Central software - edit key screen



Takeaways

PCI Security Standards Council

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

PCI Security Standards Council

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)

PCI Security Standards Council

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

PCI Security Standards Council

Security Standards Council®