MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

MINDSHARE AGENDA

GET APP

STEAL NOW, DECRYPT LATER

PROTECTION THROUGH HYBRID DISK ENCRYPTION

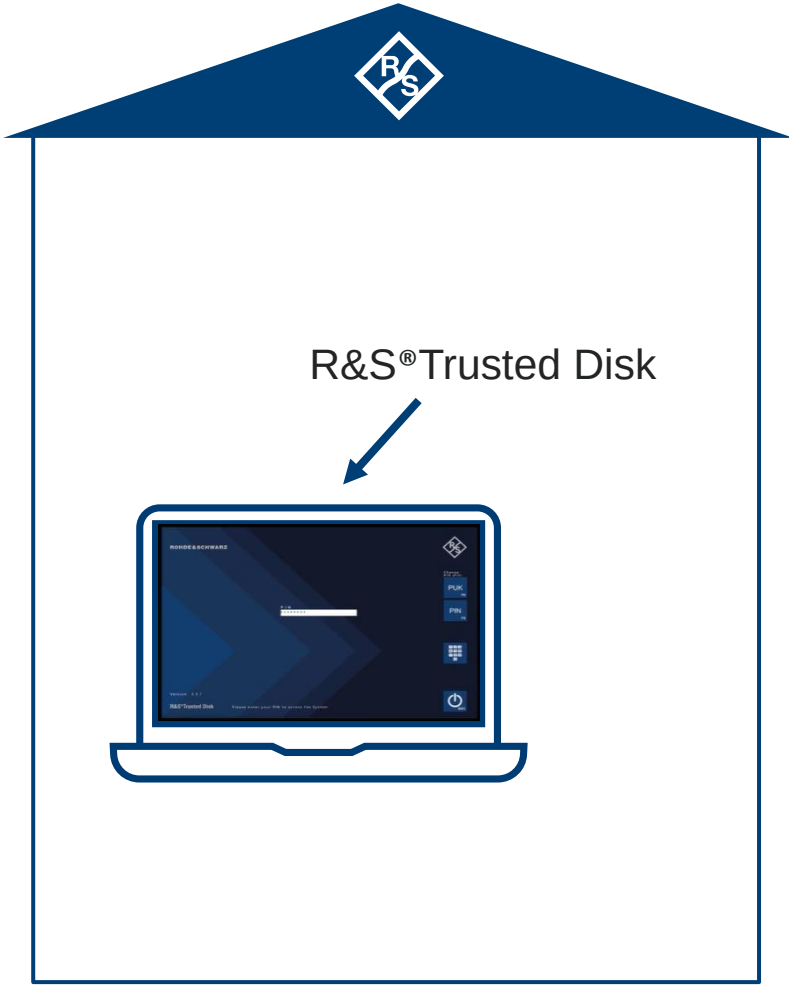
Fabian Albert - Rohde & Schwarz Cybersecurity GmbH

Mindshare 2025

ROHDE&SCHWARZ

Make ideas real

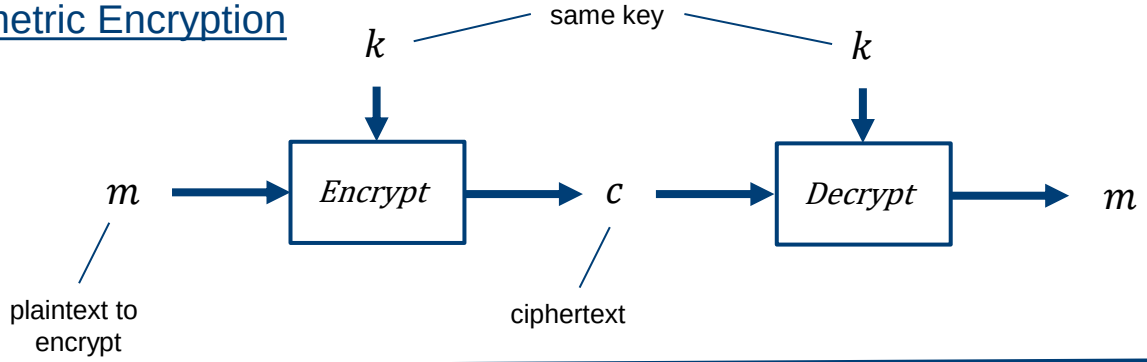
STEAL NOW – DECRYPT LATER



STEAL NOW – DECRYPT LATER

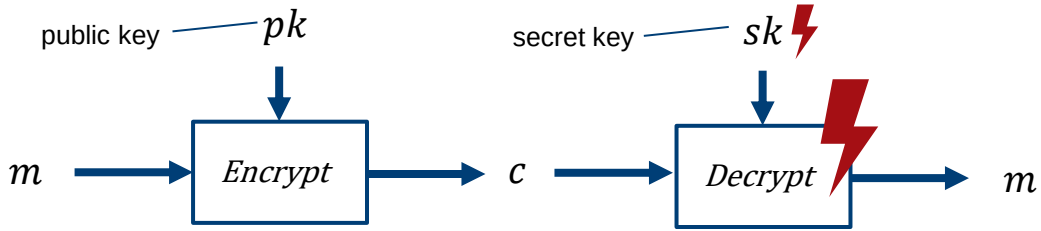
WHAT IS AFFECTED?

Symmetric Encryption



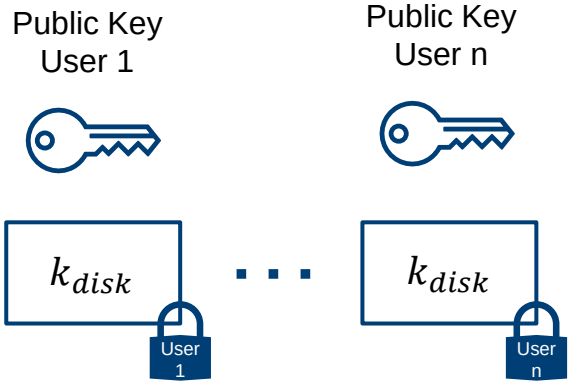
Unbroken by Quantum Computers

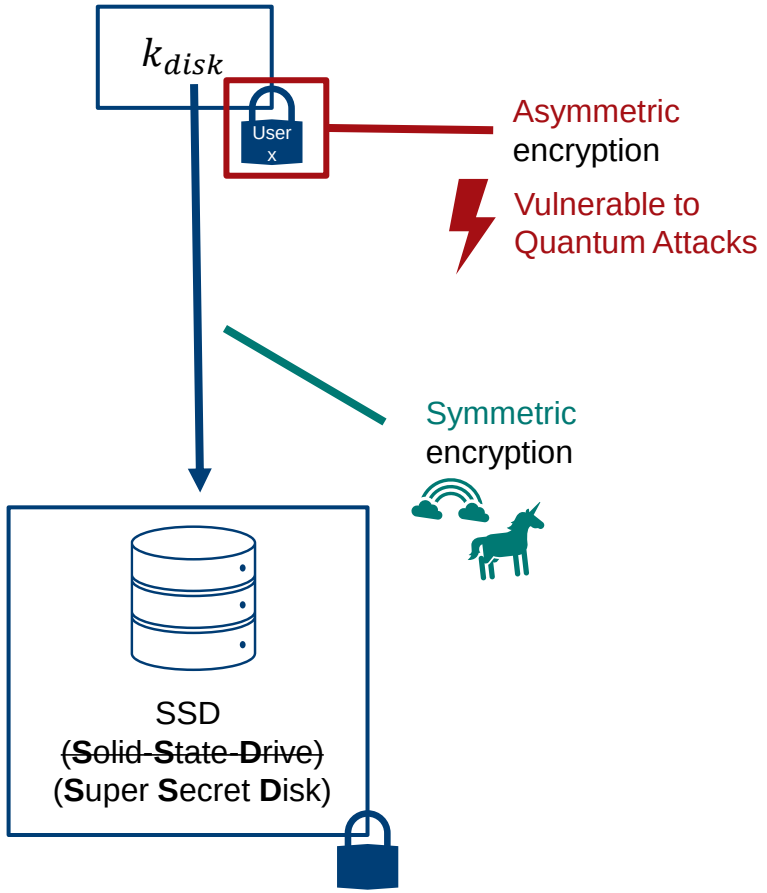
Asymmetric Encryption



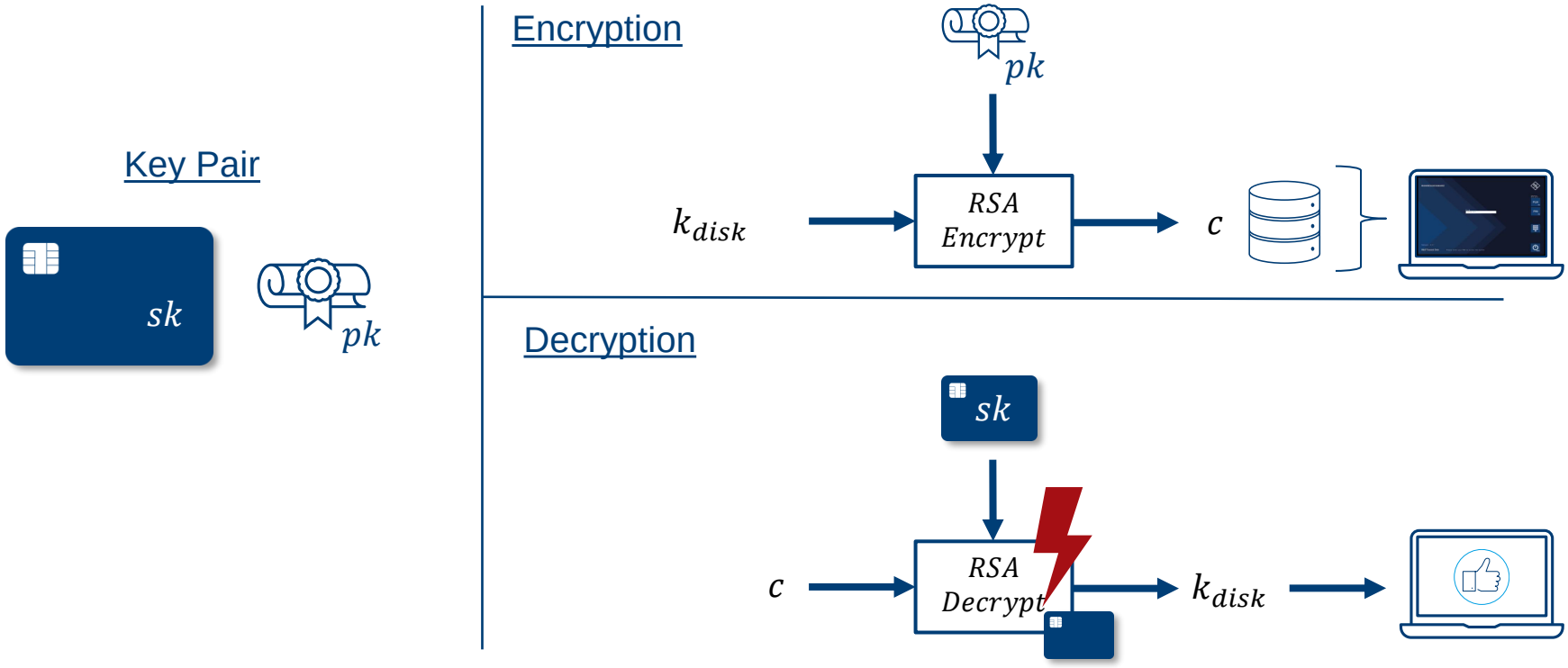
Vulnerable to Quantum Attacks

WHY CARE ABOUT PQC?





TRUSTED DISK – PK ENCRYPTION (TODAY)



FIPS 203 – ML-KEM

Short:
„ML-KEM“

recommended by

Bundesamt
für Sicherheit in der
Informationstechnik

ML-KEM SMARTCARDS

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

KRITIS3M

Bundesministerium für Wirtschaft und Energie

Operational Technology-Security in KRITIS Systems

EVIDEN

CardOS PQCLM

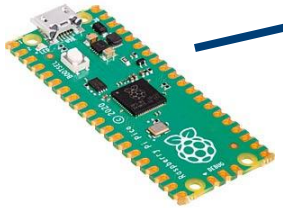
Post **Q**uantum **C**ryptography
Learning **M**achine

OASIS OPEN

PKCS #11 Specification Version 3.2

Committee Specification Working Draft 13

16 April 2025



Raspberry Pi Pico

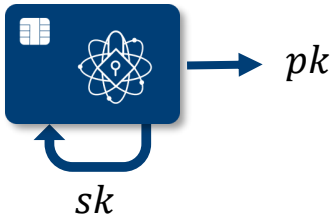
Acts as PQ-Smartcard
(ML-KEM, ML-DSA, ECC, …)

ML-KEM SMARTCARDS

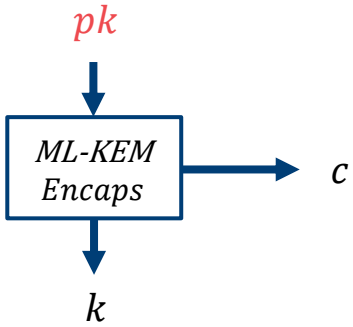
Key Gen

```
CK_MECHANISM_TYPE mechanism_type = CKM_ML_KEM_KEY_PAIR_GEN;
CK_ML_KEM_PARAMETER_SET_TYPE param_set = CKP_ML_KEM_768;
CK_ATTRIBUTE param_set_attr = {CKA_PARAMETER_SET, &param_set, sizeof(param_set)};
CK_ATTRIBUTE allow_encaps_attr = {CKA_ENCAPSULATE, &boolTrue, sizeof(CK_BBOOL)};
```

```
C_GenerateKeyPair(
      session,
      &mechanism,
      sk_template, sk_template_count,
      pk_template, pk_template_count,
      out_pk_handle, out_sk_handle);
```

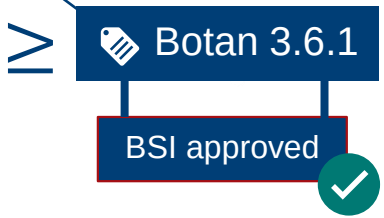


ML-KEM SMARTCARDS

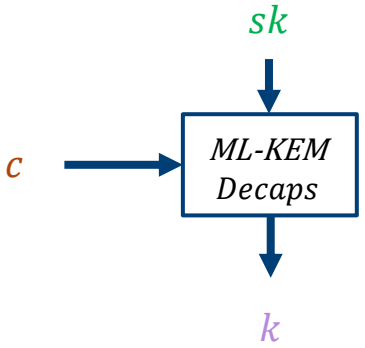


[Encapsulation]

```
Botan::ML_KEM_PublicKey pk(pk_bytes, Botan::KyberMode::Kyber768);
auto encaps = Botan::PK_KEM_Encryptor(pk, "Raw").encrypt(rng);
// -> k = encaps.shared_key(); c = encaps.encapsulated_shared_key();
```



ML-KEM SMARTCARDS

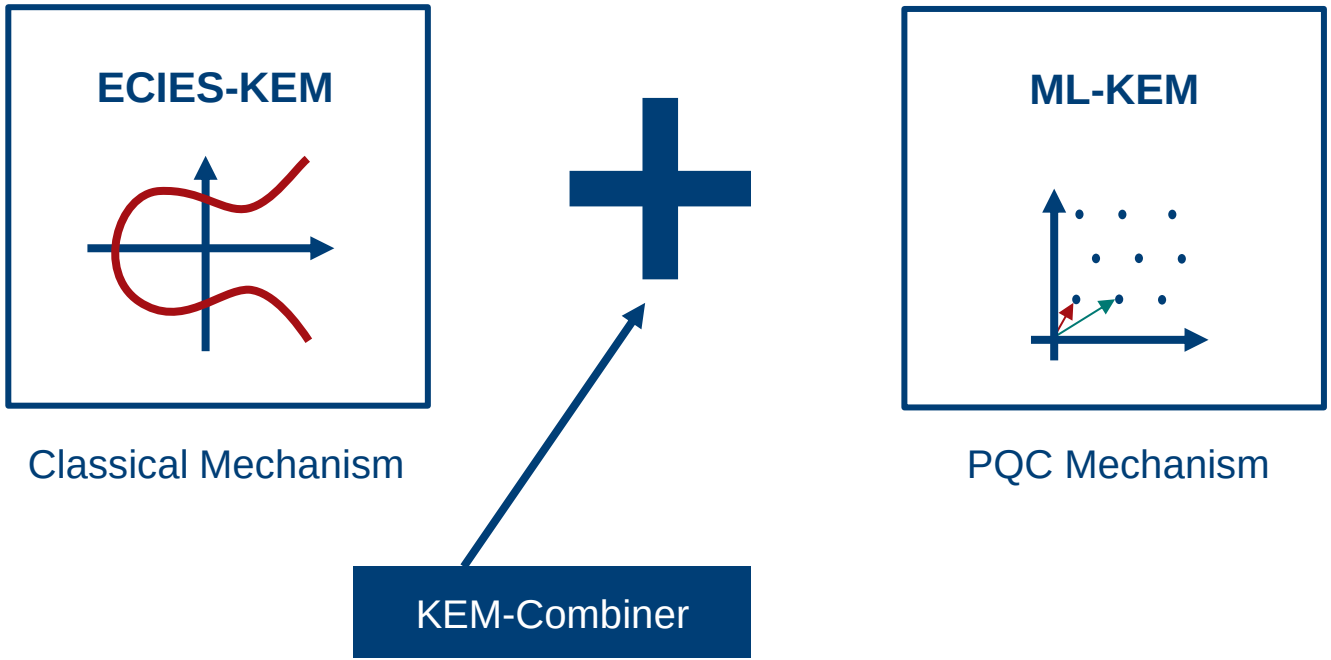


Decapsulation

```
CK_MECHANISM_TYPE mechanism_type = CKM_ML_KEM;
```

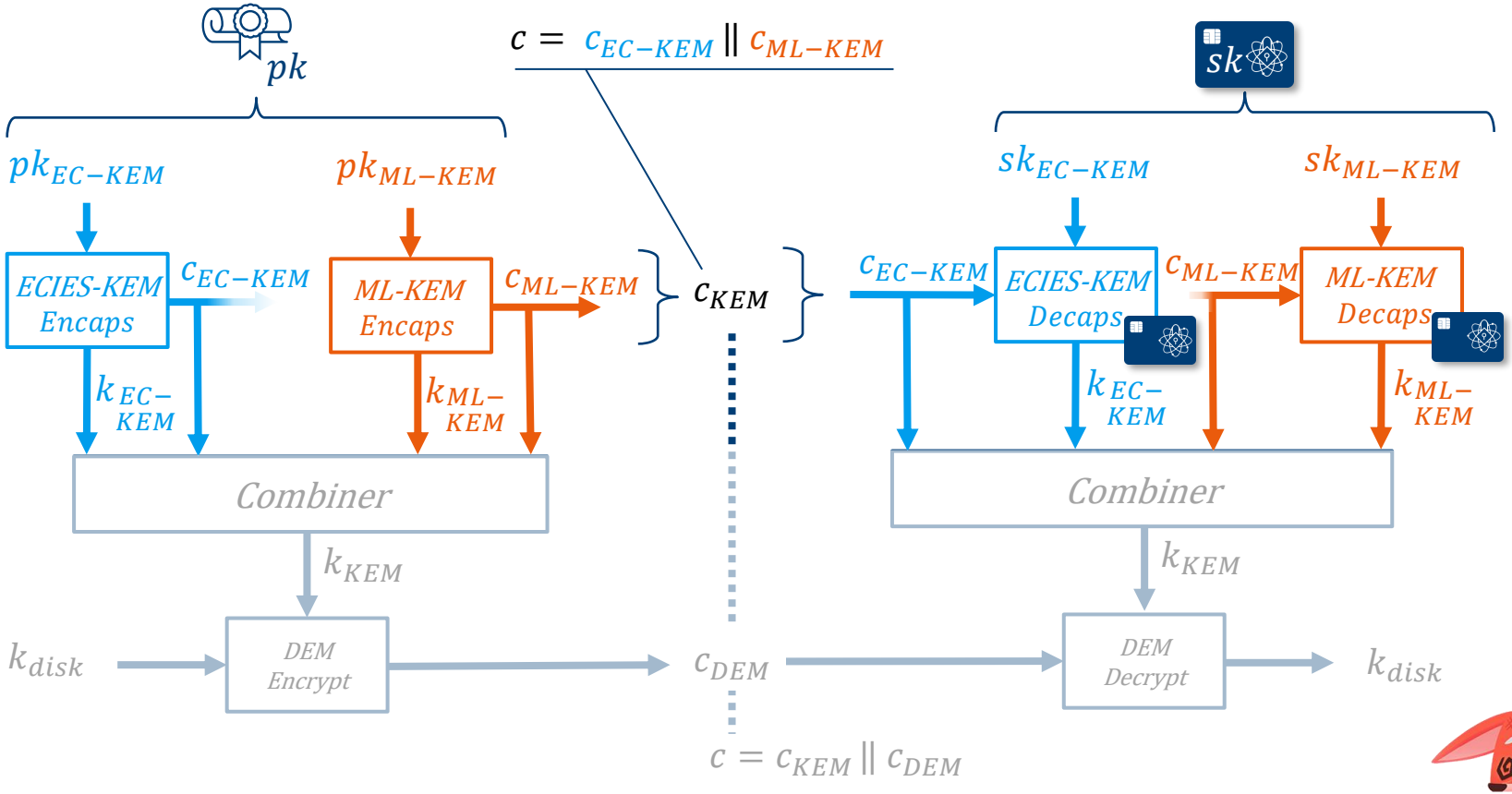
```
C_DecapsulateKey(
      session,
      mechanism,
      sk_handle,
      k_template, k_template_count,
      c_data, c_size,
      out_k_handle);
```

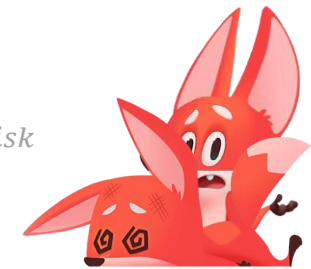
PQC TRANSITION – BEST OF BOTH WORLDS



Encryption

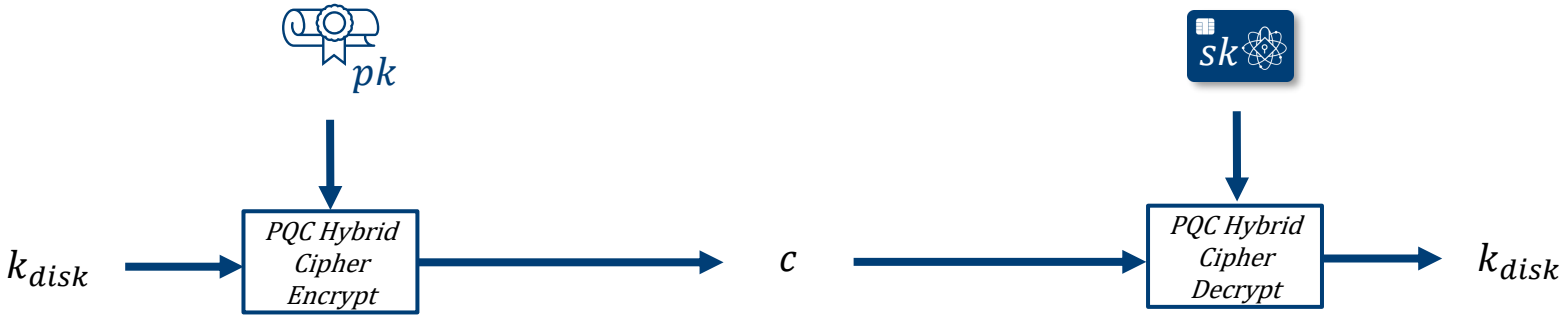
Decryption



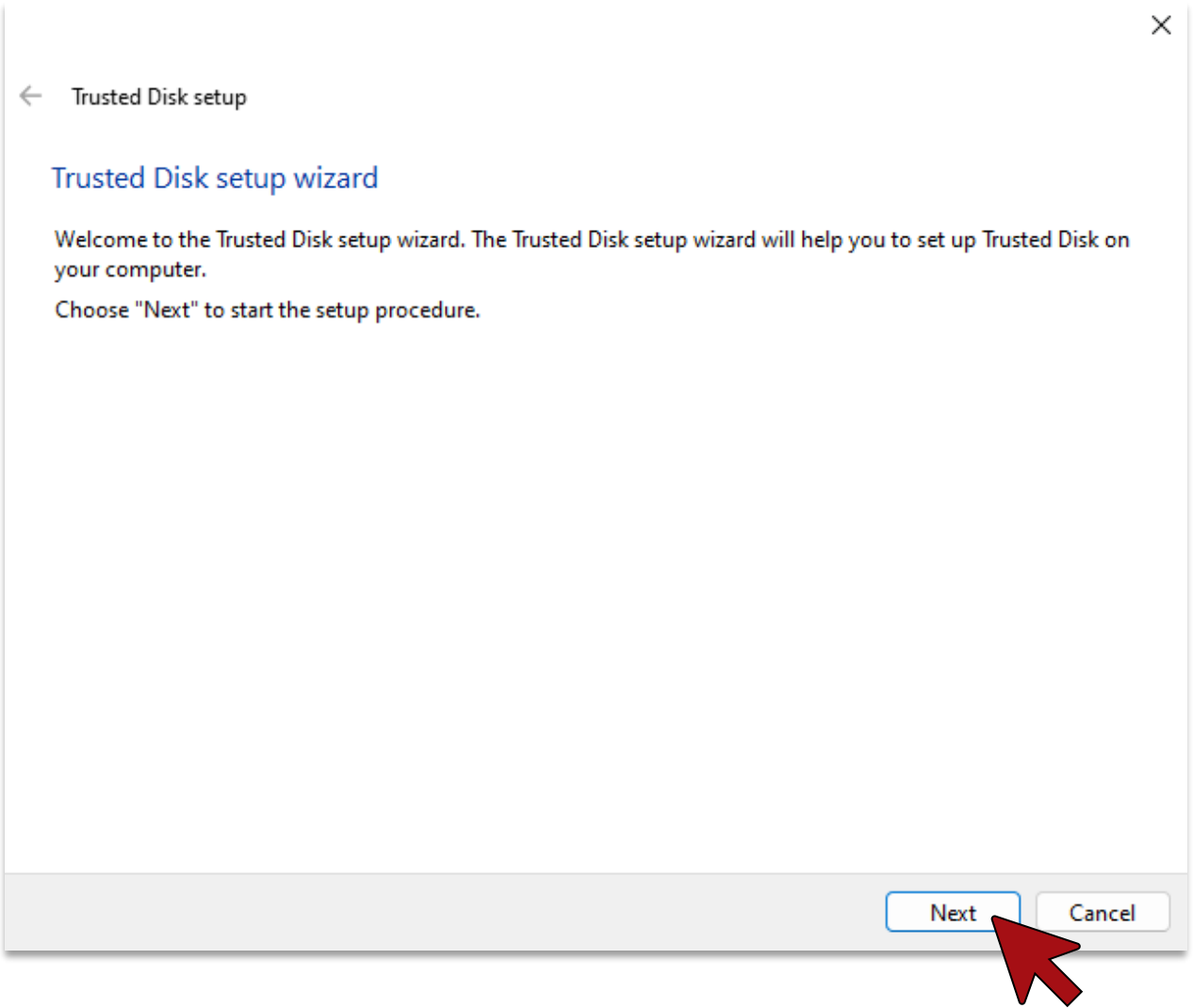


Encryption

Decryption



Demo Time


Trusted Disk setup
Trusted Disk setup wizard
Welcome to the Trusted Disk setup wizard. The Trusted Disk setup wizard will help you to set up Trusted Disk on your computer.
Choose "Next" to start the setup procedure.
Next
Cancel

Demo Time

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Valid from	Monday, January 1, 2024 2:0...
Valid to	Saturday, January 1, 2124 2:...
Subject	Test Certificate (HybridCipher...
Public key	1.3.6.1.3.65280.1.1 (0 Bits)
Key Usage	Key Encipherment (20)
Enhanced Key Usage	Unknown Key Usage (1.3.6.1....
Thumbprint	40752d602fd5da4e629e0b88f...

```
1f 96 26 6f 22 60 74 a3 8b 1f 5b 14 7d 17
98 77 f5 4e e7 41 fb 3f 81 ab 2c 2a 00 43
a9 34 25 7a 98 ce 9a ee 01 43 9e f8 86 cd
e6 49 38 9f 4c 37 fc 27 04 11 d2 01 5e df
82 70 43 68 78 df a3 a9 ac a4 cf a8 2b 5d
42 54 58 0c 4e 20 e0 e4 8e 2e a2 eb 39 99
3f f2 87 9b 02 0d 8b b1 45 6f e0 75 81 f6
eb dc fb 33 25 6d 47 1f 47 da fa 7e 63 10
f9 bf 48
```

Edit Properties... | Copy to File...

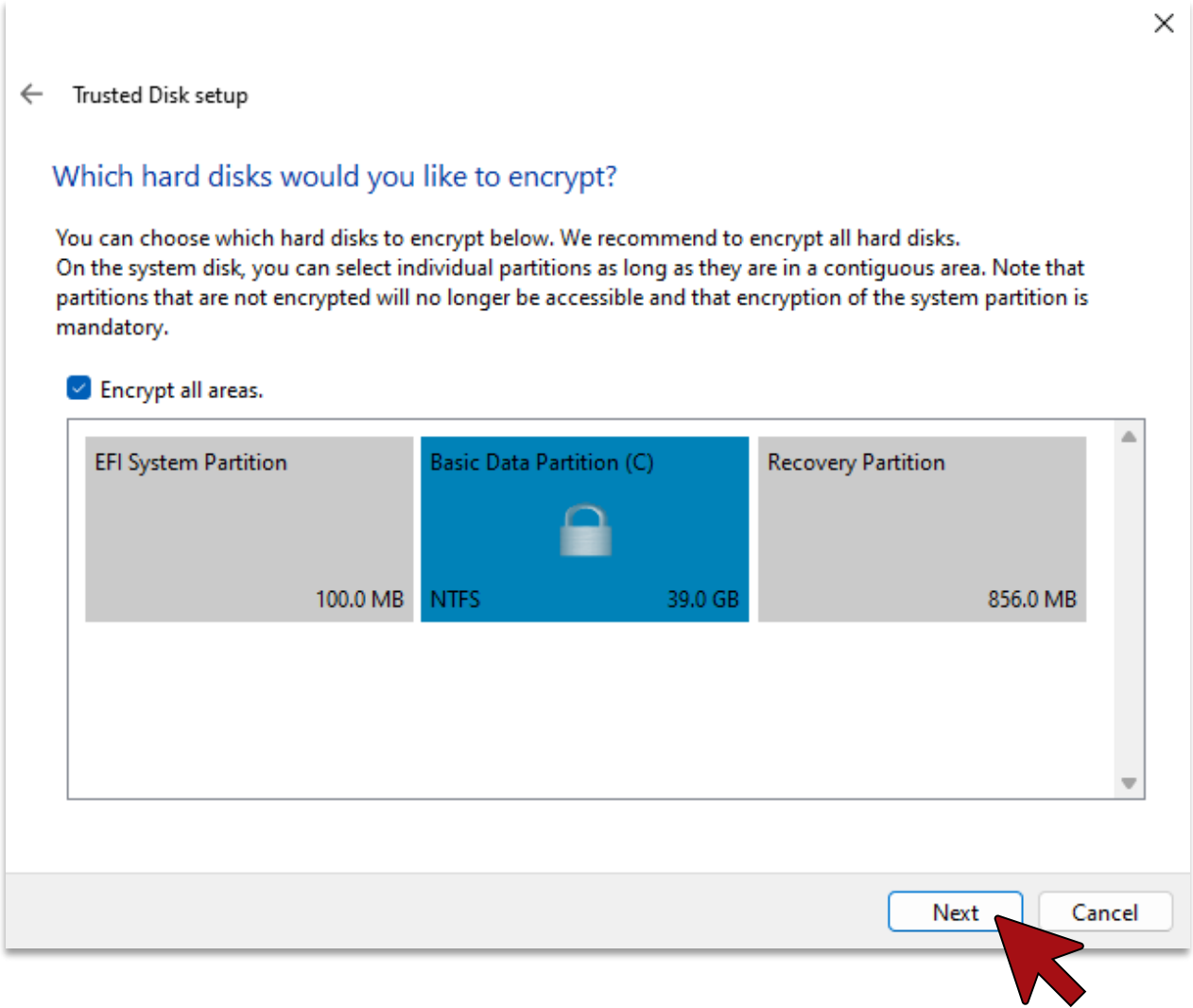
OK

...

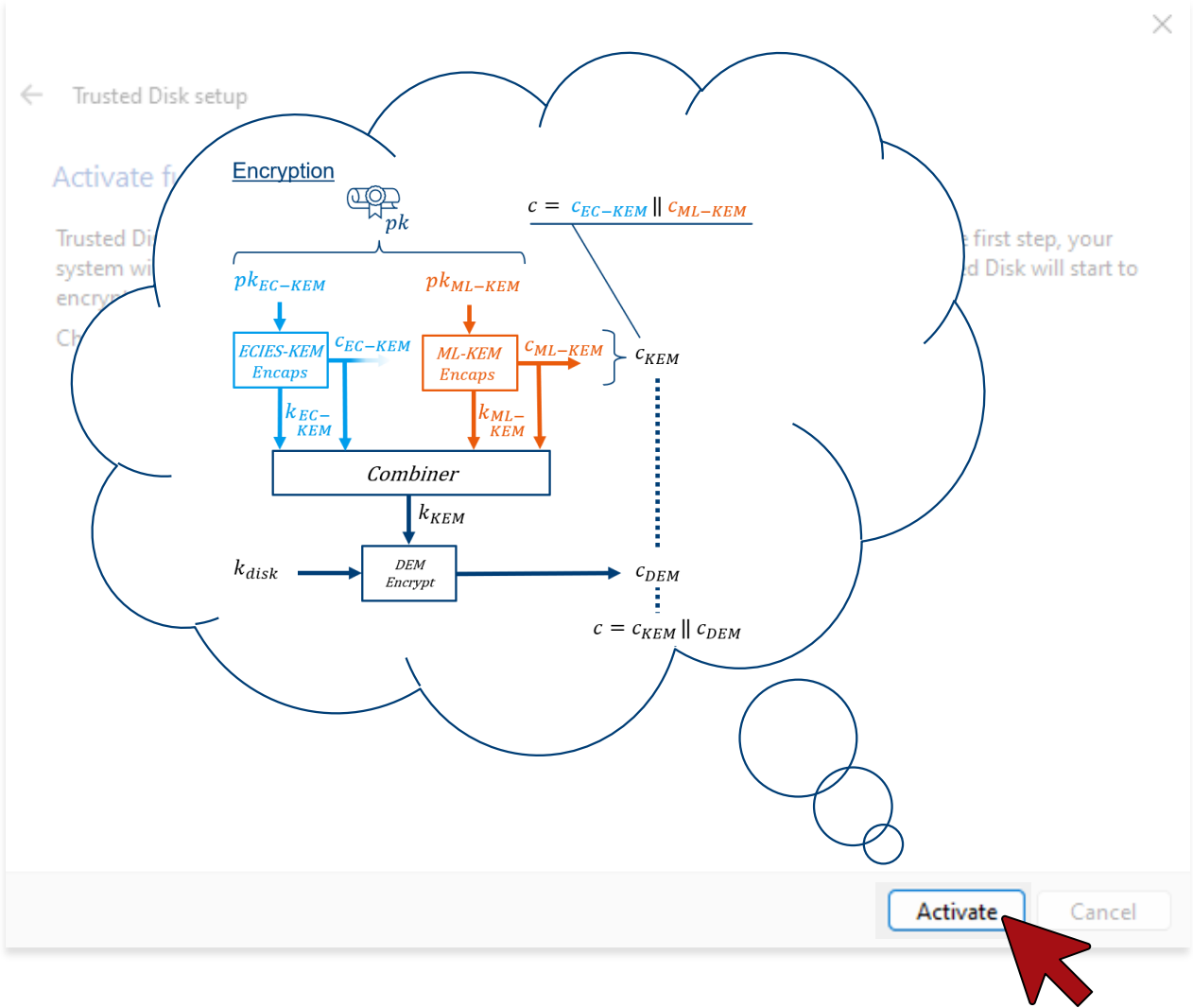
ML-KEM Public Key

EC Public Key

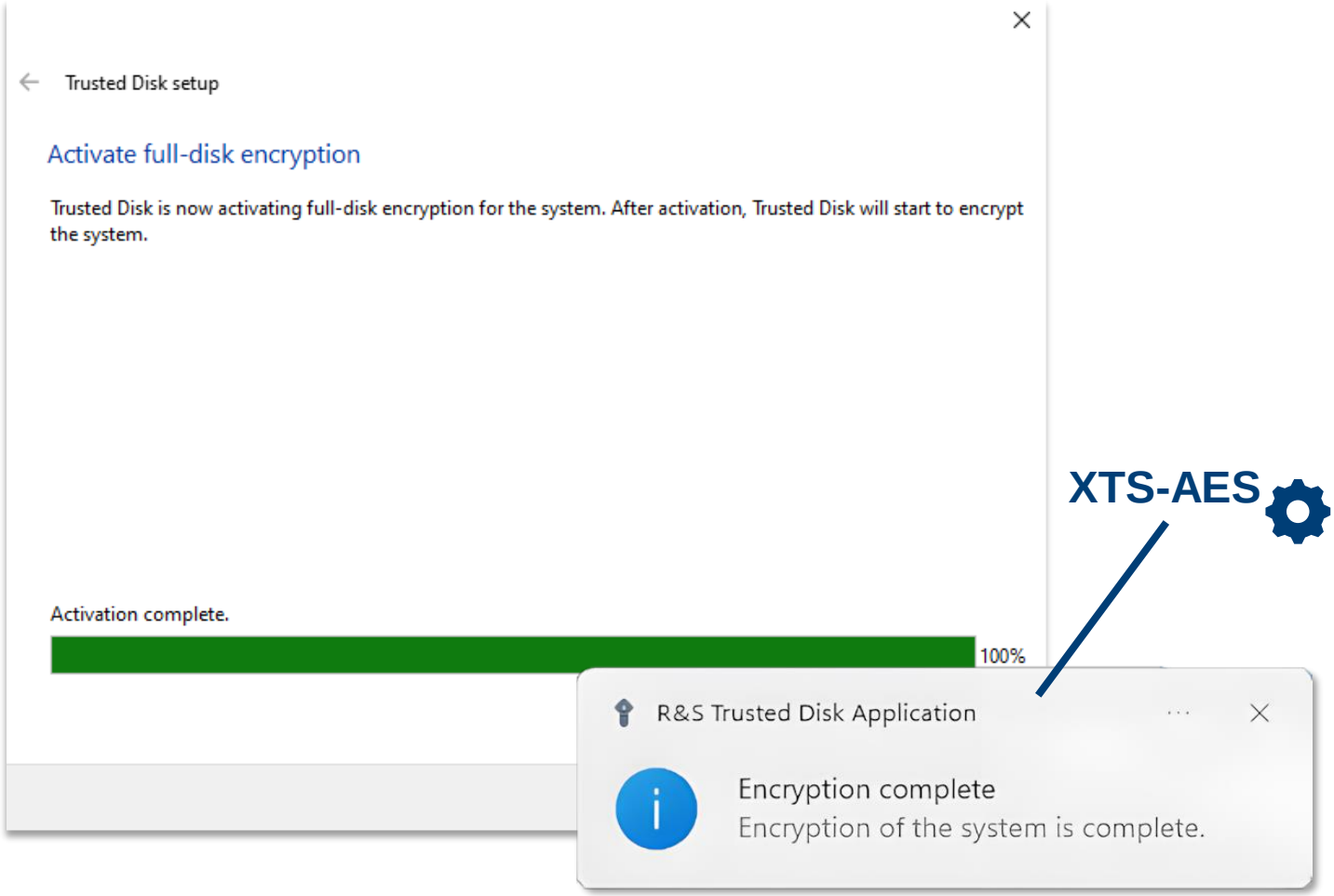
Demo Time


Trusted Disk setup
Which hard disks would you like to encrypt?
You can choose which hard disks to encrypt below. We recommend to encrypt all hard disks.
On the system disk, you can select individual partitions as long as they are in a contiguous area. Note that partitions that are not encrypted will no longer be accessible and that encryption of the system partition is mandatory.
Encrypt all areas.
EFI System Partition
100.0 MB
Basic Data Partition (C)
NTFS
39.0 GB
Recovery Partition
856.0 MB
Next
Cancel

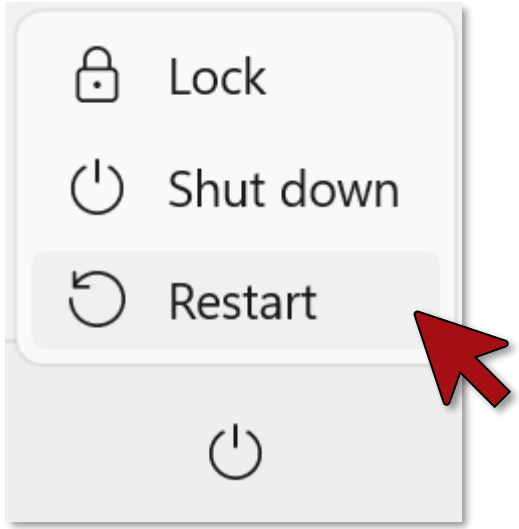
Demo Time


Trusted Disk setup
Activate f
Trusted Di
system wi
encryp
Ch
first step, your
d Disk will start to
Encryption
pk
$c = c_{EC-KEM} \| c_{ML-KEM}$
pk_{EC-KEM}
pk_{ML-KEM}
ECIES-KEM Encaps
c_{EC-KEM}
ML-KEM Encaps
c_{ML-KEM}
c_{KEM}
k_{EC-KEM}
k_{ML-KEM}
Combiner
k_{KEM}
k_{disk}
DEM Encrypt
c_{DEM}
$c = c_{KEM} \| c_{DEM}$
Activate
Cancel

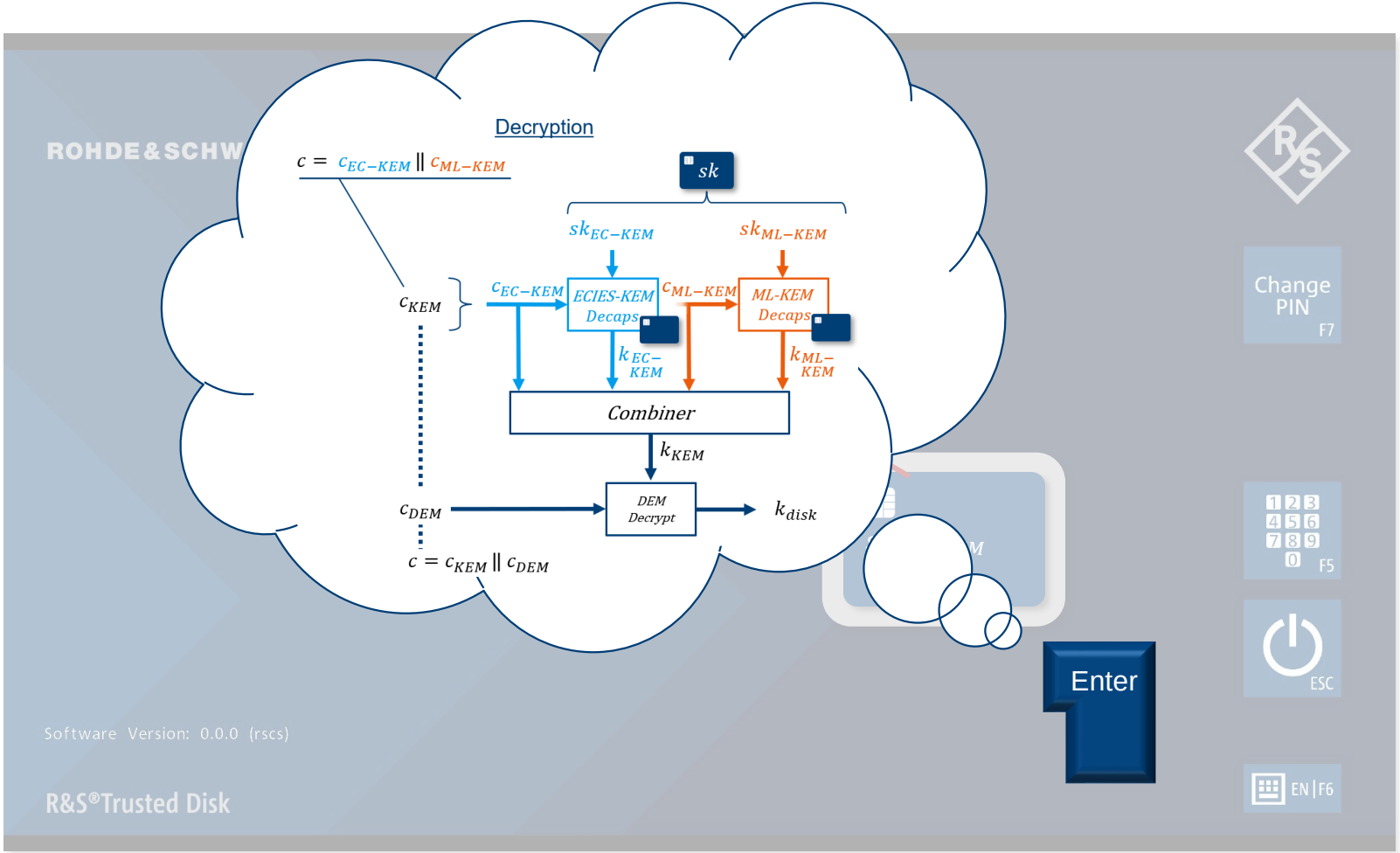
Demo Time


Trusted Disk setup
Activate full-disk encryption
Trusted Disk is now activating full-disk encryption for the system. After activation, Trusted Disk will start to encrypt the system.
Activation complete.
100%
XTS-AES
R&S Trusted Disk Application
Encryption complete
Encryption of the system is complete.

Reboot Time

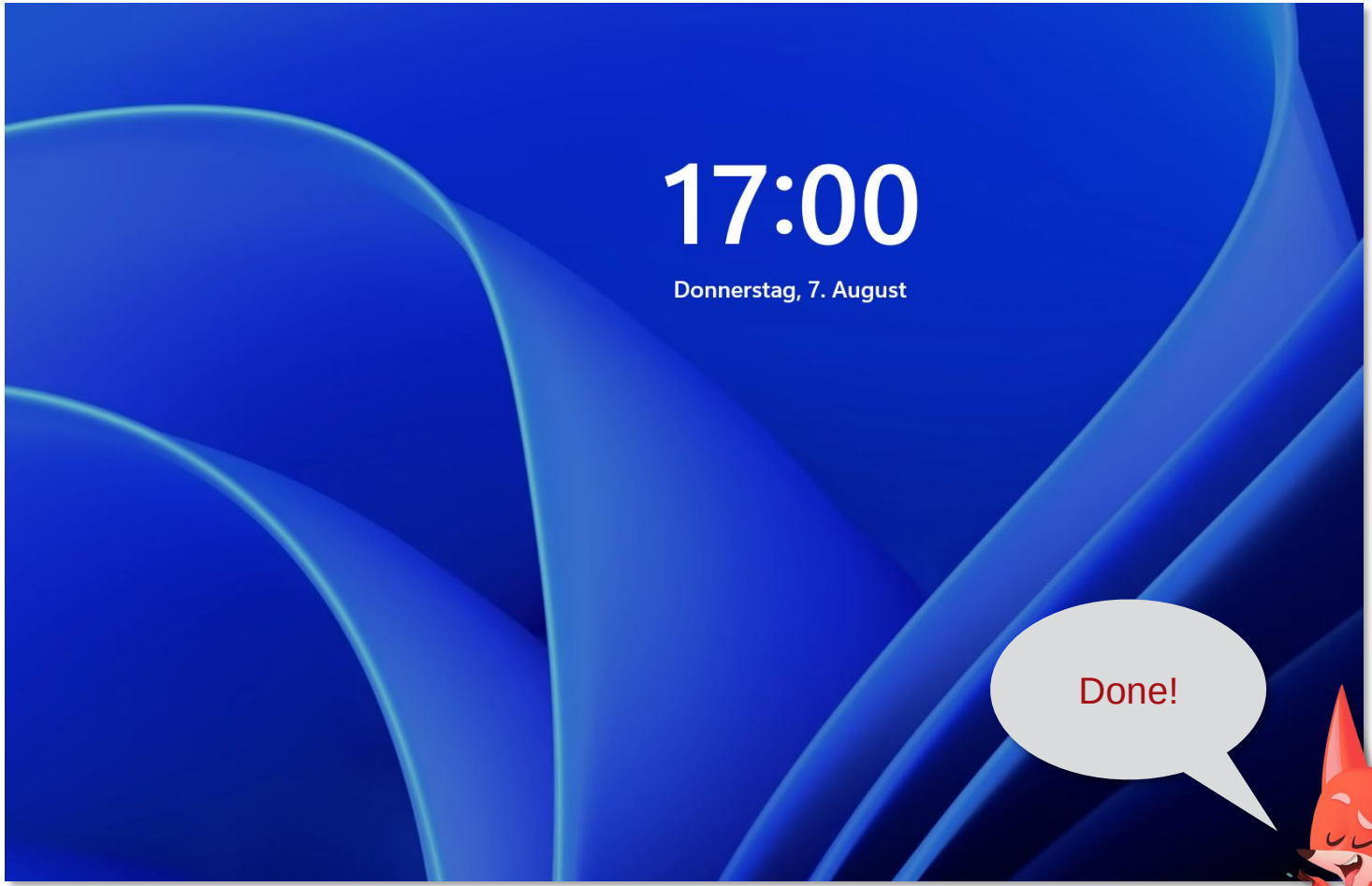


Demo Time


ROHDE&SCHW
Decryption
$c = c_{EC-KEM} \| c_{ML-KEM}$
sk
sk_{EC-KEM}
sk_{ML-KEM}
c_{KEM}
c_{EC-KEM}
ECIES-KEM Decaps
c_{ML-KEM}
ML-KEM Decaps
k_{EC-KEM}
k_{ML-KEM}
Combiner
k_{KEM}
c_{DEM}
DEM Decrypt
k_{disk}
$c = c_{KEM} \| c_{DEM}$
Change PIN F7
F5
ESC
Enter
EN | F6
Software Version: 0.0.0 (rscs)
R&S®Trusted Disk

Demo Time

Demo Time



THANKS FOR YOUR ATTENTION!

ANY QUESTIONS?

?

Fabian Albert

Development Engineer

fabian.albert@rohde-schwarz.com

@FAlbertDev

PQC, Trusted Disk, Botan Development

BACKUP-SLIDES

DEMO TIME

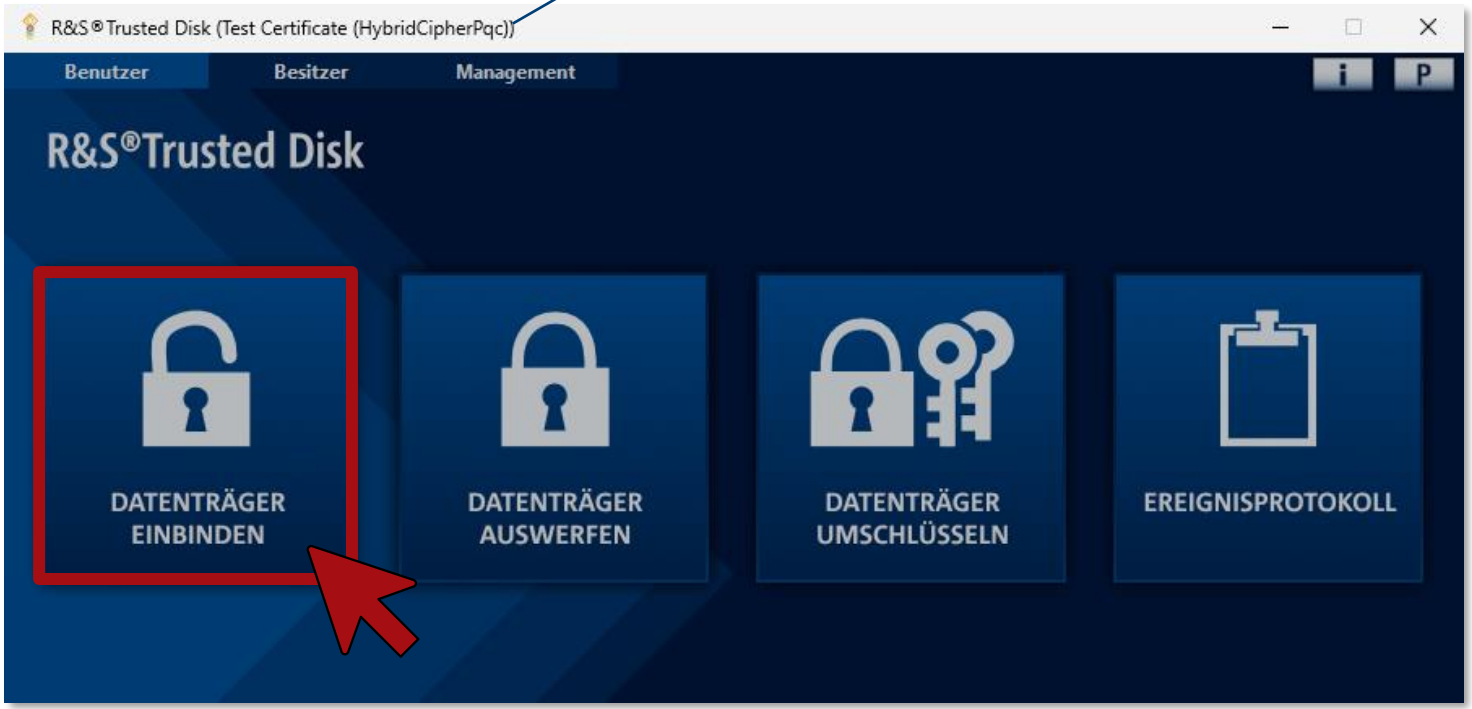
User Certificate with
Combined Key
(ECIES-KEM + ML-KEM)

DEMO TIME

User Certificate with Combined Key (ECIES-KEM + ML-KEM)

DEMO TIME

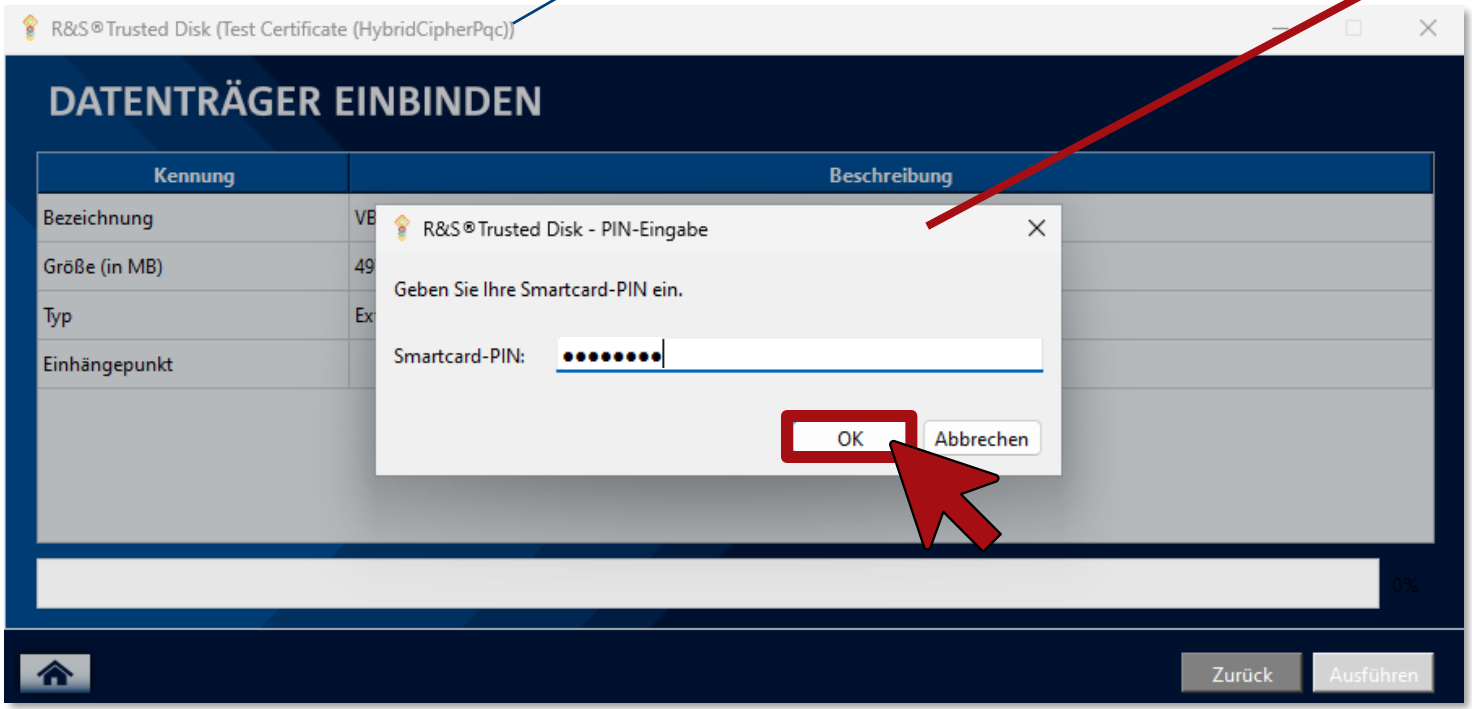
User Certificate with
Combined Key
(ECIES-KEM + ML-KEM)



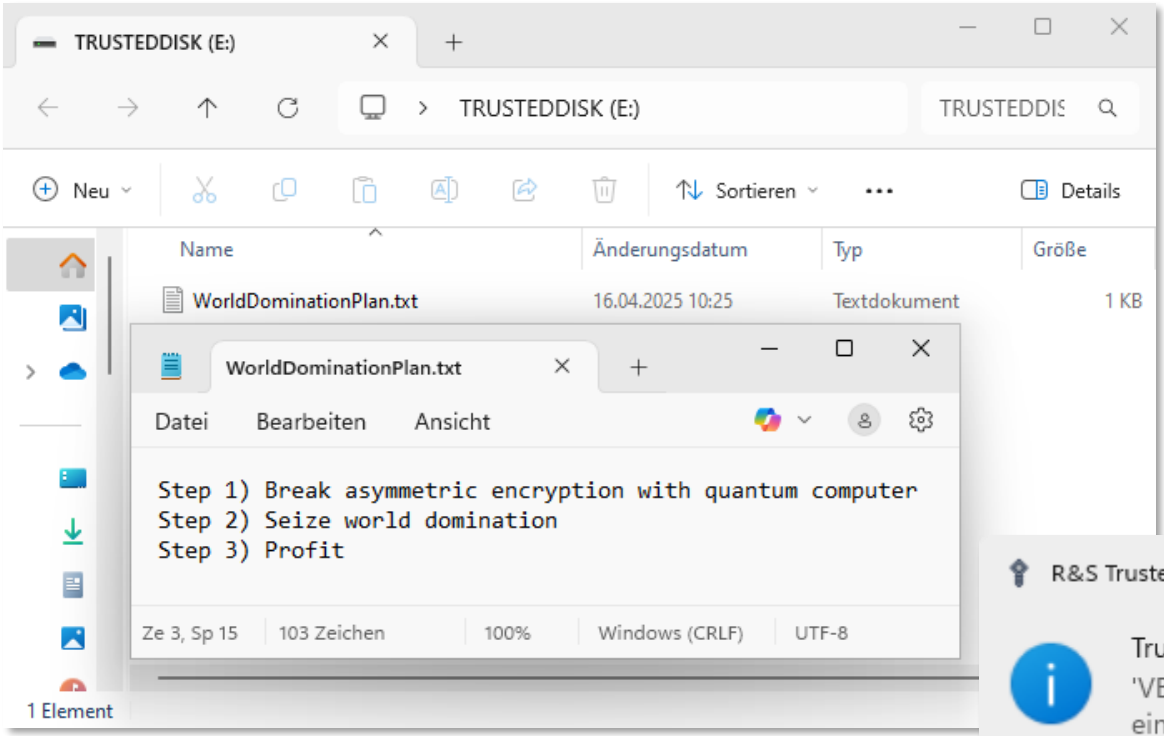
DEMO TIME

User Certificate with
Combined Key
(ECIES-KEM + ML-KEM)

$sk_{ECIES-KEM}$
sk_{ML-KEM}



DEMO TIME


TRUSTEDDISK (E:)
TRUSTEDDISK (E:)
TRUSTEDDIS
Neu
Sortieren
Details
Name
Änderungsdatum
Typ
Größe
WorldDominationPlan.txt
16.04.2025 10:25
Textdokument
1 KB
WorldDominationPlan.txt
Datei
Bearbeiten
Ansicht
Step 1) Break asymmetric encryption with quantum computer
Step 2) Seize world domination
Step 3) Profit
Ze 3, Sp 15
103 Zeichen
100%
Windows (CRLF)
UTF-8
1 Element


R&S Trusted Disk Application
Trusted Disk Datenträger eingebunden
'VBOX HARDDISK USB Device' wurde eingehängt als 'E: (TRUSTEDDISK)'.

MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

TAKE A MINUTE AND GIVE US FEEDBACK