Post-Quantum

Cryptography Conference

Hybrid PQC E-Mail Communication: Easing Migration Pain

Secure e-mail communication is a natural fit for hybrid cryptography, offering long-term confidentiality and non-repudiation for users. This talk introduces a prototype system comprising a Certificate Authority, Certificate Management System, and an extended Open Source client application, including an integration module for Microsoft Outlook. The presentation explores the selection criteria for hybrid schemes and the rationale behind choosing Composite and ICA approaches to facilitate PKI and S/MIME migration. It also shares insights from implementing and using pure PQC, Composite, and ICA hybrid constructions. Topics include certificate creation, client enrollment, and securely signing and encrypting e-mail messages using S/MIME across various cryptographic configurations, emphasizing the hybrid integration of classical and post-quantum secure cryptography.

Jan Klaußner

Senior Product Architect at Bundesdruckerei GmbH

SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

January 15 and 16, 2025 - Austin, TX (US) | Online

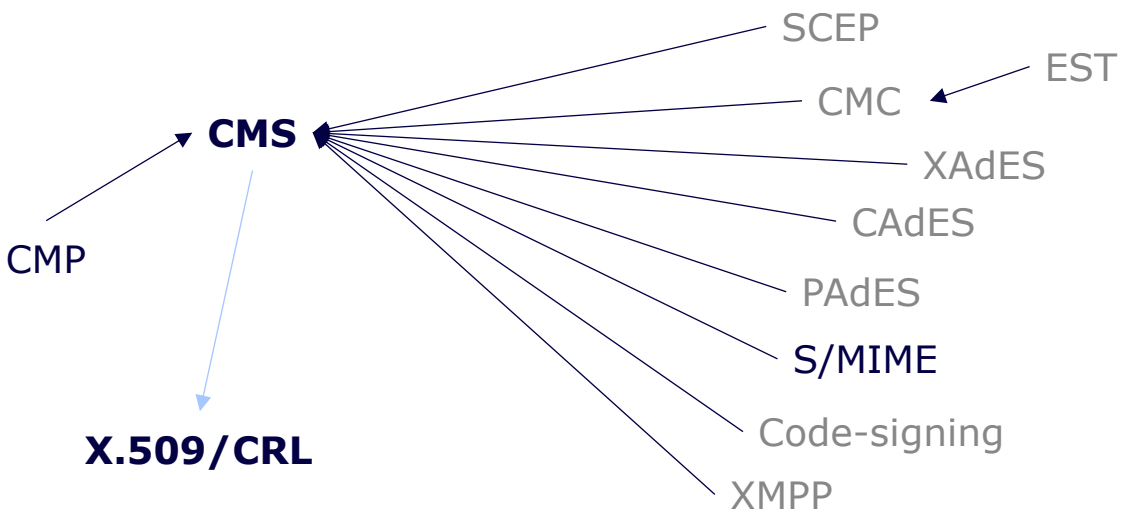
Hybrid PQC E-Mail Communication

Easing Migration Pain

Date 15/01/2025
Location PKI Consortium – PQC Conference
Author Jan Klaussner

Why E-Mail?

Cryptographic Dependencies
(non-exhaustive)



- **S/MIME uses CMS for cryptography**
- **CMS is used in many other protocols**
- **Almost all also use X.509 certificates**
- **Migrating CMS solves issue for all others**

PQC E-Mail - Goals

- **Prototype targets agencies and businesses**
- **Use case which is widely used in real world application**
- **Usage of S/MIME**
- **Integration in Microsoft Outlook (Windows)**
- **FOSS**

Interesting sidenote: In specific configurations, the FOSS we modified is currently to secure classified information

The Inevitable - Hybrids

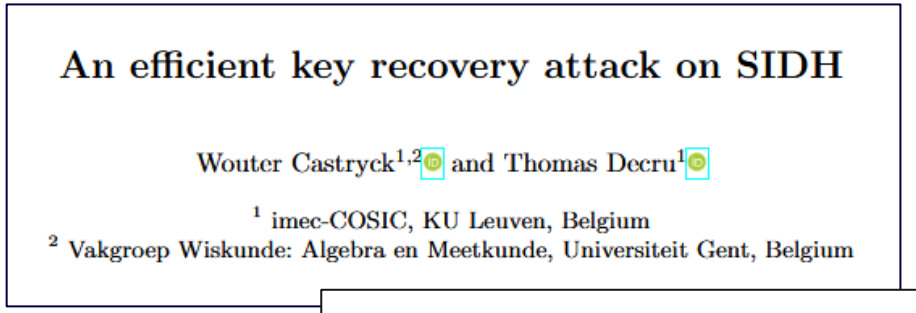
BSI, ANSSI et al. require combination of classic and PQC mechanisms[1]

Trust in Mathematical Security?

New approaches still need more review (see SIKE)

Trust in Implementation?

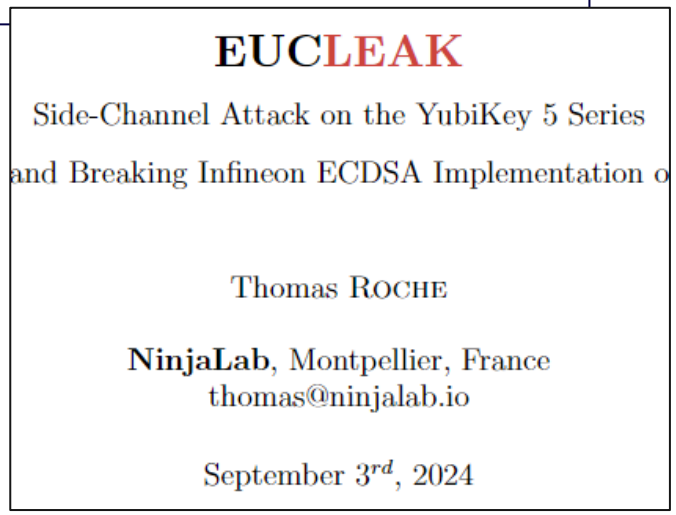
New complex algorithms prone to implementation faults (see EUCLEAK)



An efficient key recovery attack on SIDH

Wouter Castryck[1,2] and Thomas Decru[1]

[1] imec-COSIC, KU Leuven, Belgium
[2] Vakgroep Wiskunde: Algebra en Meetkunde, Universiteit Gent, Belgium



EUCLEAK

Side-Channel Attack on the YubiKey 5 Series

and Breaking Infineon ECDSA Implementation o

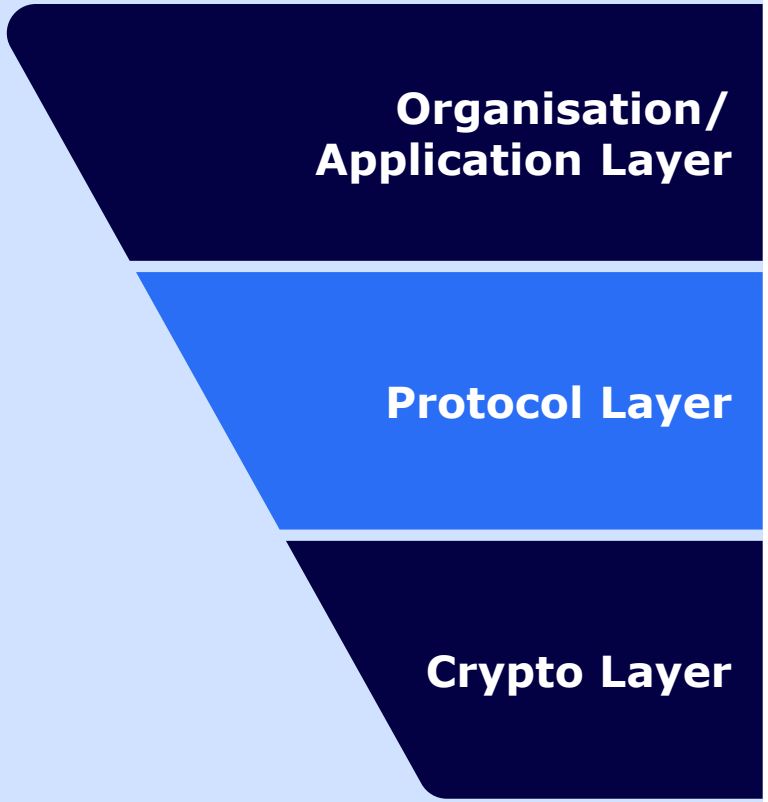
Thomas Roche

NinjaLab, Montpellier, France
thomas@ninjalab.io

September 3rd, 2024

[1] ENISA "Postquantum cryptography: integration study" 2022; for Germany: BSI (Federal Office for Information Security) "*Migration to Post Quantum Cryptography: Recommendations for action by the BSI*, ver.1.0, 31 May 2021; France: ANSSI "ANSSI views on the Post-Quantum Cryptography transition", 30 March 2022; Spain: Centro Criptografico ´ Nacional, "*CCN-TEC 009. Recommendations for a safe post-quantum transition*" (2022).

How to Hybrid



Needs additional user interaction

e.g. Parallel PKIs, Double Signing

High effort, high chance of errors

Solution for every Protocol and Service

Every Protocol with own flavor

Synchronization is hard, "Adapter" required

Algorithm as combination of algorithms

Can be used directly in all Protocols without friction

How to Hybrid
in Protocols

Organisation/ Application Layer

Protocol Layer

Crypto Layer

Encryption

Hybrid not possible with existing standards/drafts

Signatures

Counter Signatures in CMS (RFC-5652)

Multiple Signatures in CMS (RFC-5752)

Certificates

X.509 Isara Catalyst (ITU-T X.509 10/2019)

Related Certificates (draft-ietf-lamps-cert-binding-for-multi-auth)

How to Hybrid
in Protocols

Organisation/ Application Layer

Protocol Layer

Crypto Layer

Encryption

Hybrid not possible with existing standards/

Signatures

Counter Signatures in CMS (RFC-5652)

Multiple Signatures in CMS (RFC-5752)

Certificates

X.509 Isara Catalyst (ITU-T X.509 10/2019)

Related Certificates (draft-ietf-lamps-cert-binding-for-multi-auth)

How to Hybrid in Protocols

Organisation/ Application Layer

Protocol Layer

Crypto Layer

Encryption

Hybrid not possible with existing standards/drafts

Signatures

Counter Signatures in CMS (RFC-5652)

Multiple Signatures in CMS (RFC-5752)

non-hierarchical, linked signatures

Certificates

X.509 Isara Catalyst (ITU-T X.509 10/2019)

Related Certificates (draft-ietf-lamps-cert-binding-for-multi-auth)

How to Hybrid
in Protocols

Organisation/ Application Layer

Protocol Layer

Crypto Layer

Encryption

Hybrid not possible with existing standards/drafts

Signatures

Counter Signatures in CMS (RFC-5652)

Multiple Signatures in CMS (RFC-5752)

one additional key/signature as X.509 extension

Certificates

X.509 Isara Catalyst (ITU-T X.509 10/2019)

Related Certificates (draft-ietf-lamps-cert-binding-for-multi-auth)

How to Hybrid
in Protocols

Organisation/ Application Layer

Protocol Layer

Crypto Layer

Encryption

Hybrid not possible with existing standards/drafts

Signatures

Counter Signatures in CMS (RFC-5652)

Multiple Signatures in CMS (RFC-5752)

Certificates

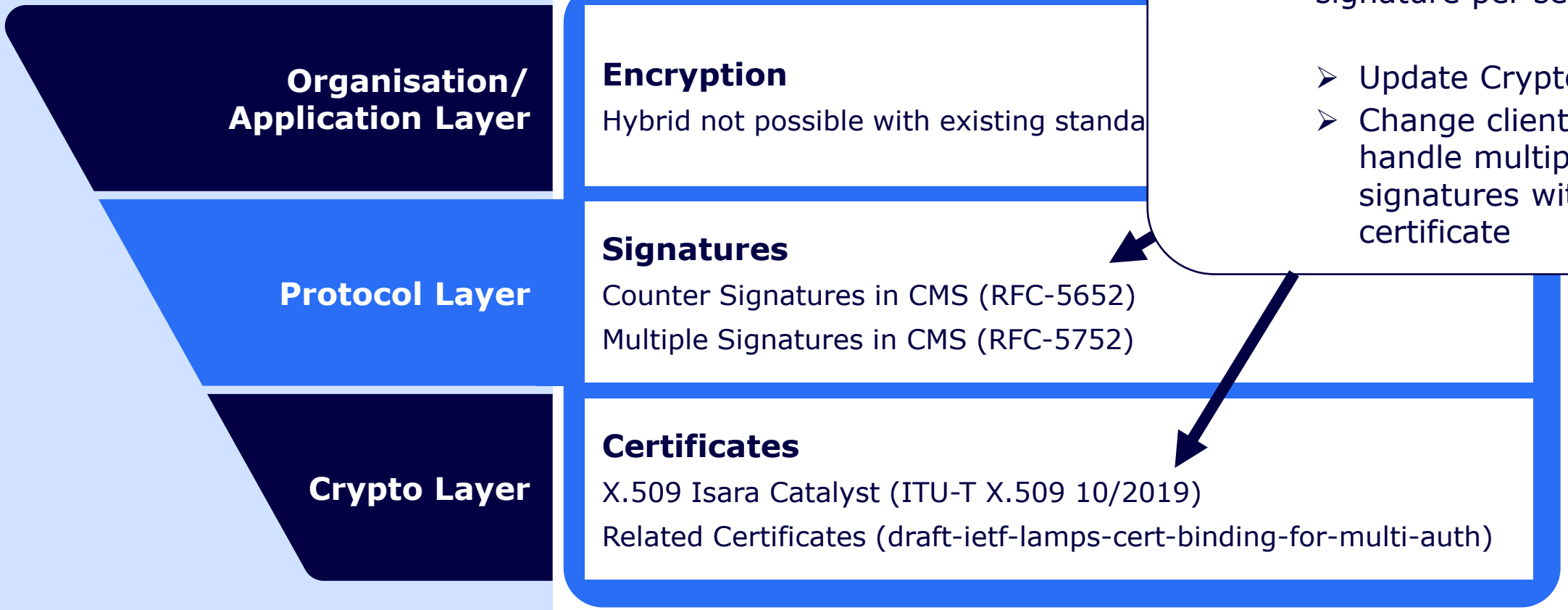
X.509 Isara Catalyst (ITU-T X.509 10/2019)

Related Certificates (draft-ietf-lamps-cert-binding-for-multi-auth)

two certificates linked cryptographically by X.509 extension

How to Hybrid in Protocols

How to Hybrid in Protocols

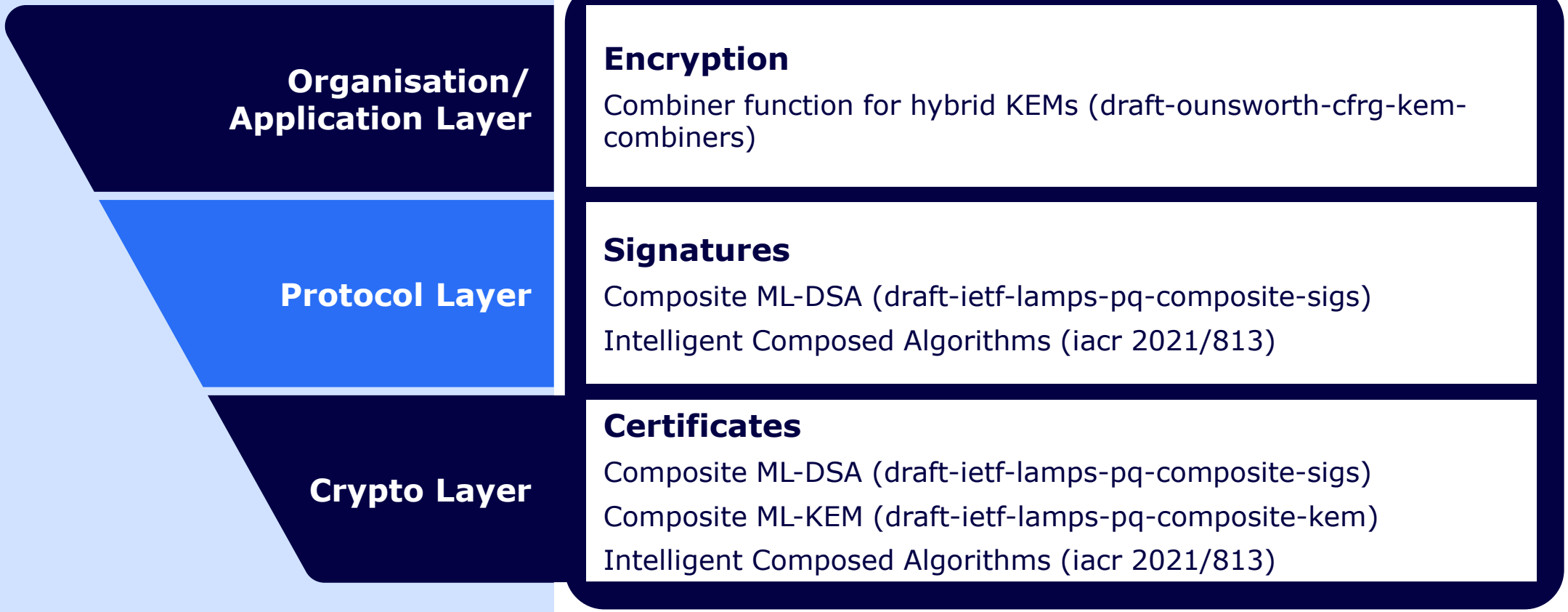


Hybrid PQC in Protocol Layer - Example

"The experimentation presented several challenges. Firstly, there were issues with the mail server processing a new email format. Existing email plugins, policies, or anti-malware systems might modify message headers or block emails due to unrecognised formats. Some systems may even issue warnings to recipients about unknown senders. These issues stemmed from the hybridised S/MIME content type and attachment extensions, leading to downstream complications."

Securing digital communications between the Banque de France & the Monetary Authority of Singapore Quantum-safe experiment report, November, 2024

How to Hybrid
in Crypto Layer



How to Hybrid
in Crypto Layer

Organisation/ Application Layer

Protocol Layer

Crypto Layer

Encryption

Combiner function for hybrid KEMs (draft-ounsworth-cfrg-kem-combiners)

Signatures

Composite ML-DSA (draft-ietf-lam

Intelligent Composed Algorithms (iacr 2021/813)

Certificates

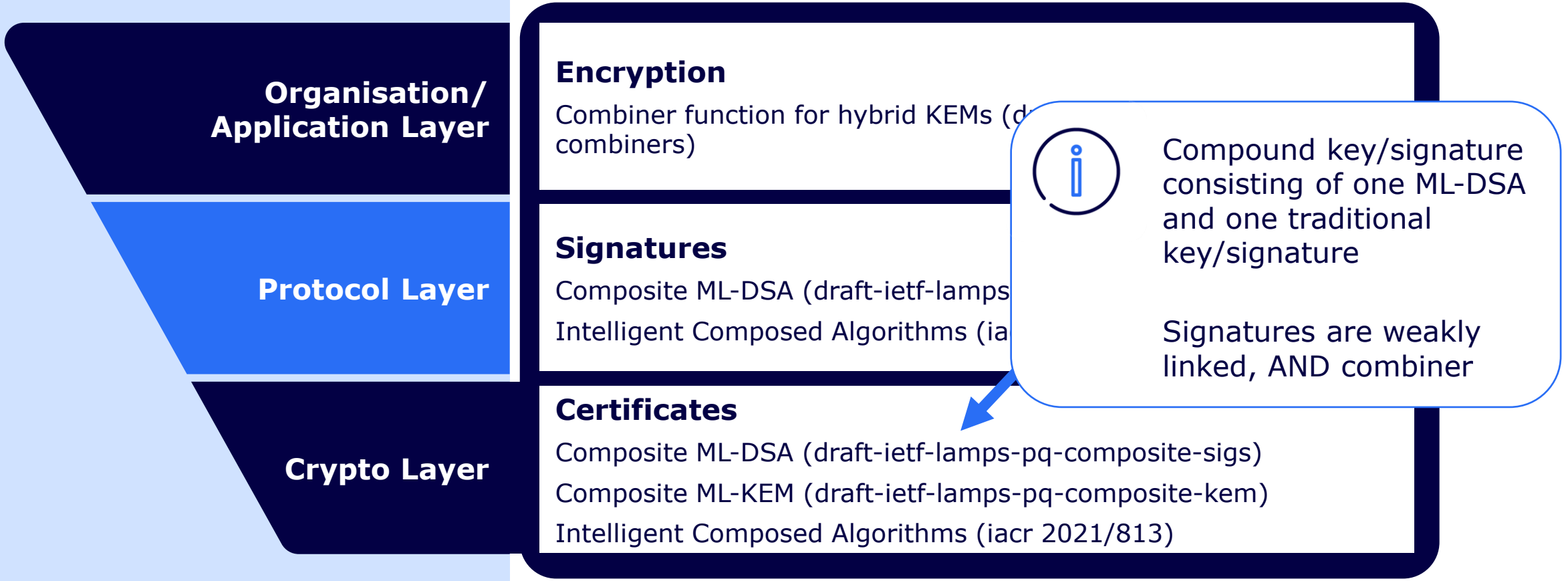
Composite ML-DSA (draft-ietf-lamps-pq-composite-sigs)

Composite ML-KEM (draft-ietf-lamps-pq-composite-kem)

Intelligent Composed Algorithms (iacr 2021/813)

Combine arbitrary number of keys to one

How to Hybrid
in Crypto Layer



How to Hybrid
in Crypto Layer

Organisation/ Application Layer

Protocol Layer

Crypto Layer

Encryption

Combiner function for hybrid KEMs (draft-ounsworth-cfrg-kem-combiners)

Signatures

Composite ML-DSA (draft-ietf-lamp

Intelligent Composed Algorithms (i

Certificates

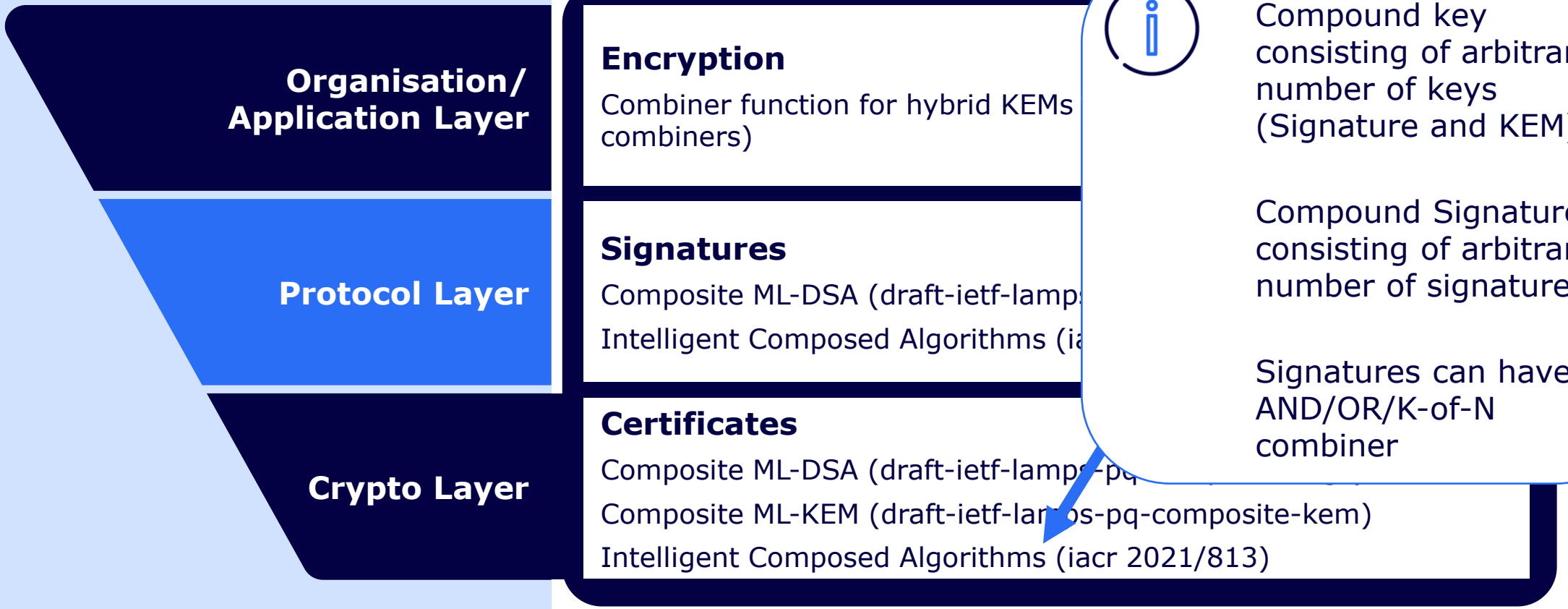
Composite ML-DSA (draft-ietf-lam s-pq-composite-sigs)

Composite ML-KEM (draft-ietf-lamps-pq-composite-kem)

Intelligent Composed Algorithms (iacr 2021/813)

Compound key consisting of one ML-KEM and one traditional key

How to Hybrid
in Crypto Layer



How to Hybrid
in Crypto Layer

Organisation/ Application Layer

Protocol Layer

Crypto Layer

Encryption

Combiner function for hybrid KEMs (
combiners)

Signatures

Composite ML-DSA (draft-ietf-lamps-pq-composite-sigs)

Intelligent Composed Algorithms (iacr 2021/813)

Certificates

Composite ML-DSA (draft-ietf-lamps-pq-composite-sigs)

Composite ML-KEM (draft-ietf-lamps-pq-composite-kem)

Intelligent Composed Algorithms (iacr 2021/813)

No significant changes
in e-mail-client required

➢ Update Crypto-Lib

bundesdruckerei.

PQC Mail Client

bundesdruckerei.

PQC Integration for MS-Outlook
Microsoft Cryptography API: Next Generation

system wide integration of proprietary signature and encryption modules
by mapping of OID to DLL with standardized ABI

+

other native applications and tools are PQ-safe (e.g. AD, Edge, Word, VPN)

—

no access to algorithm parameters

no modification outside crypto module possible > no CMS parsing for KEMs

PQC Integration for MS-Outlook
GNU Privacy Guard

integration via Outlook plugin

GnuPG-components also in other operating systems usable

usable for existing GnuPG VSDesktop for classified communication

additional installation

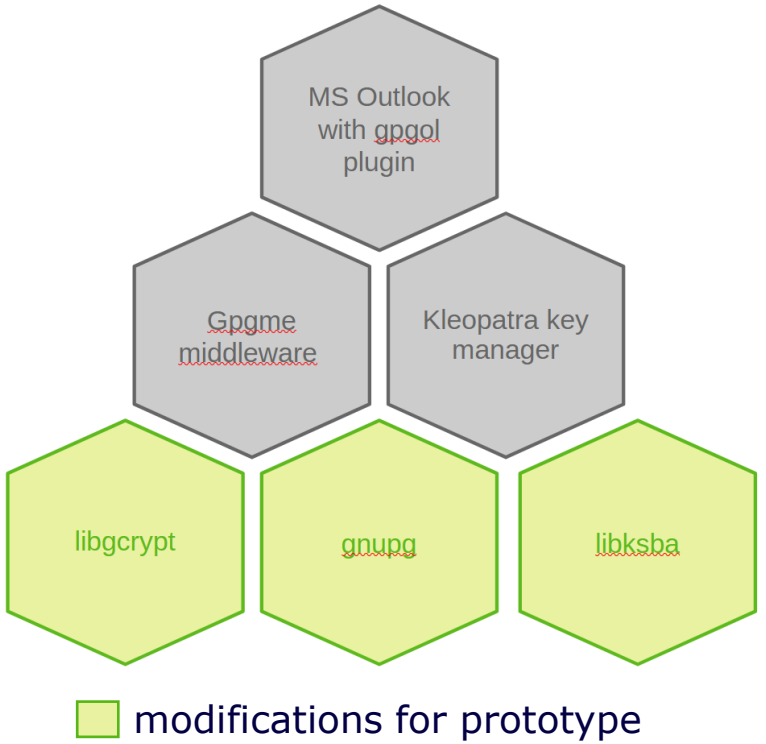
Post Quantum Secure E-Mail Client
S/MIME Implementation based on GnuPG

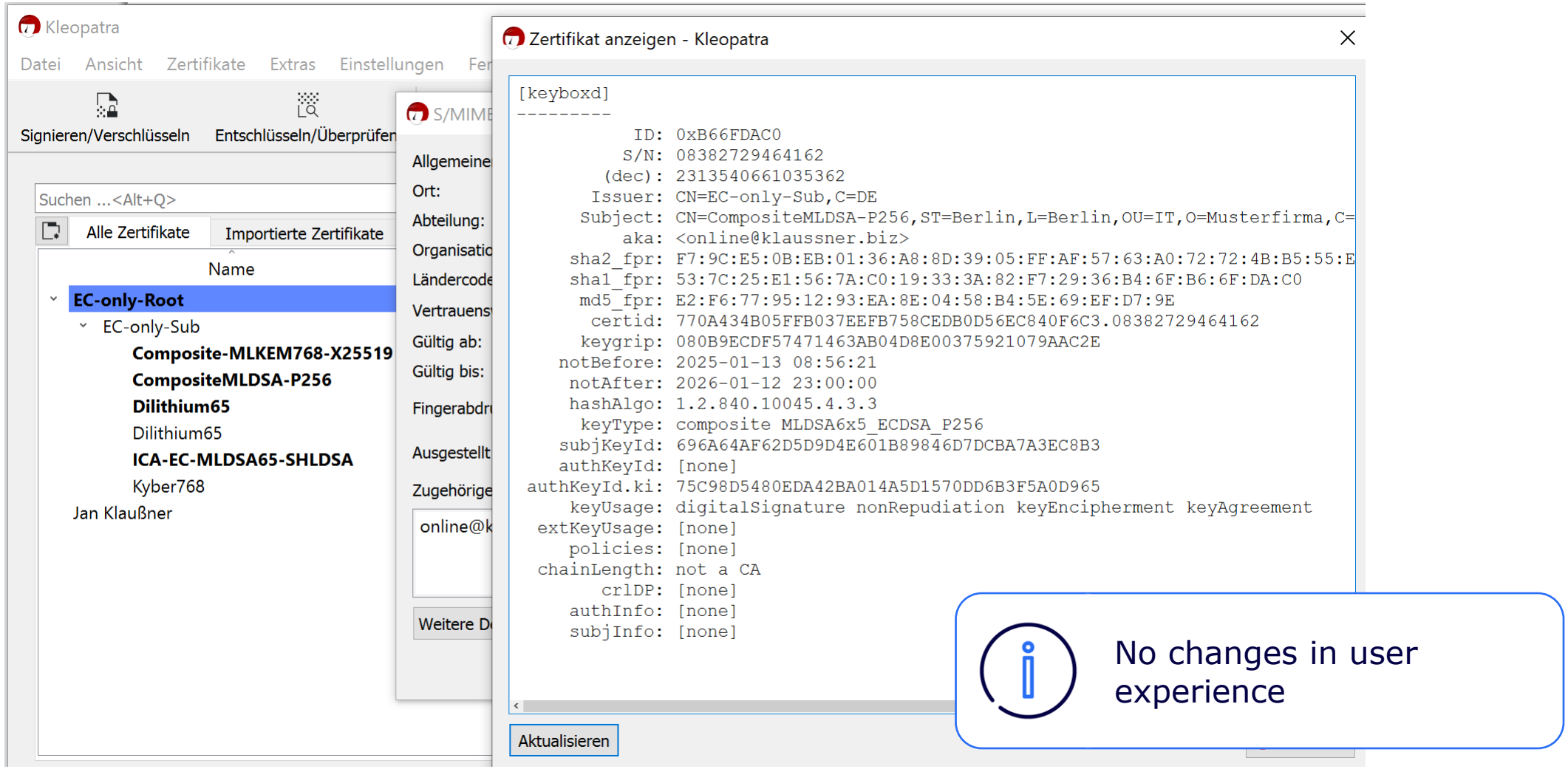
Achieved

- ✓ tested plugin for Microsoft Outlook
- ✓ certificate/key import in Kleopatra (PKCS#12)
- ✓ file encryption/signature via Kleopatra
- ✓ X.509/CMS parsing: Composites, ICAs, Single
- ✓ low level integration of liboqs (PQC cryptolib)
- ✓ User Application does not need to change

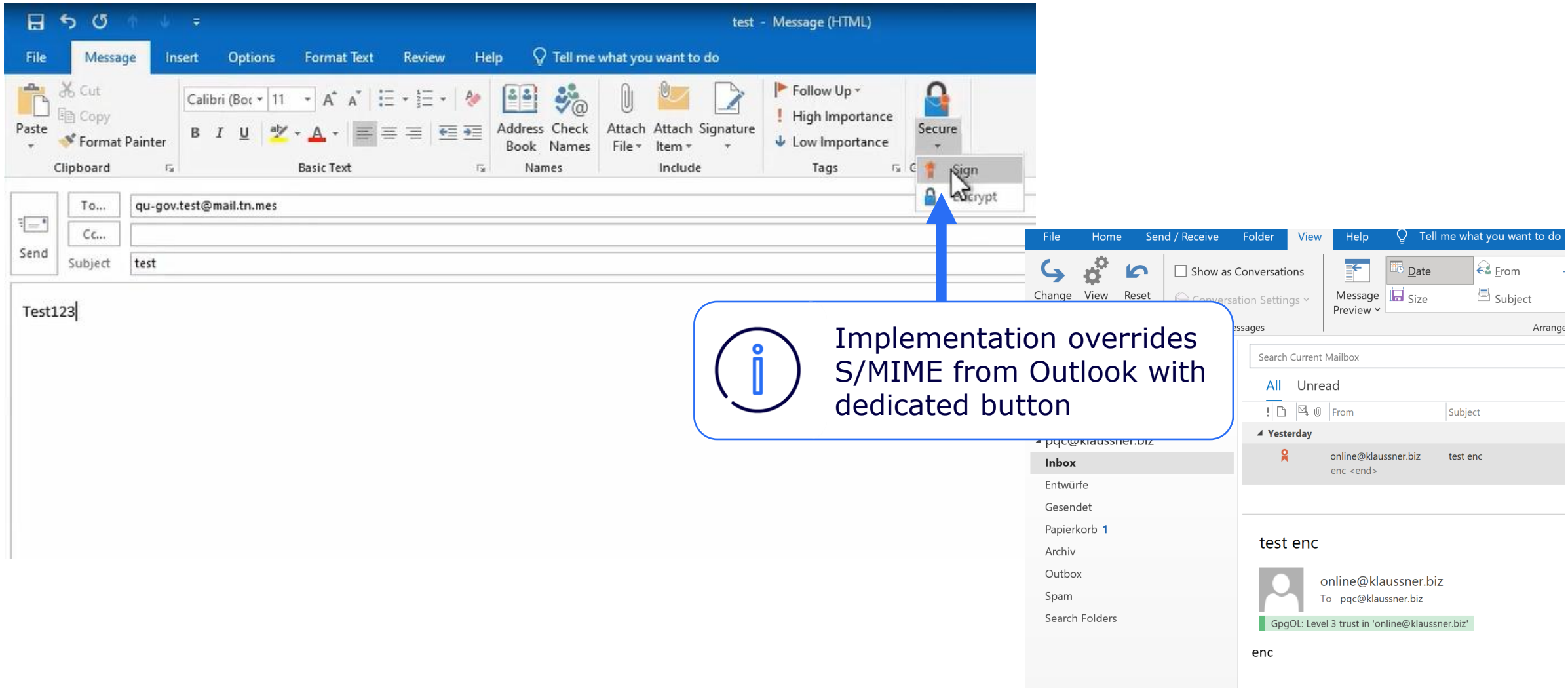
Open topics

- combine Signature and KEM keys in one certificate
- FOSS release by Bundesdruckerei



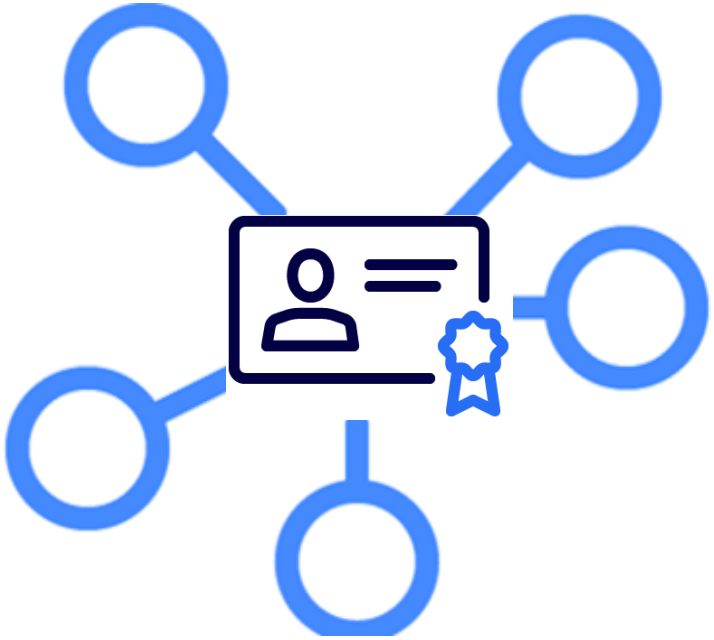

Kleopatra
Datei Ansicht Zertifikate Extras Einstellungen Fen
Signieren/Verschlüsseln
Entschlüsseln/Überprüfen
Suchen ...<Alt+Q>
Alle Zertifikate
Importierte Zertifikate
Name
EC-only-Root
EC-only-Sub
Composite-MLKEM768-X25519
CompositeMLDSA-P256
Dilithium65
Dilithium65
ICA-EC-MLDSA65-SHLDSA
Kyber768
Jan Klaußner
S/MIME
Allgemeine
Ort:
Abteilung:
Organisatio
Ländercode
Vertrauens
Gültig ab:
Gültig bis:
Fingerabdr
Ausgestellt
Zugehörige
online@k
Weitere D
Zertifikat anzeigen - Kleopatra
[keyboxd]

ID: 0xB66FDAC0
S/N: 08382729464162
(dec): 2313540661035362
Issuer: CN=EC-only-Sub,C=DE
Subject: CN=CompositeMLDSA-P256,ST=Berlin,L=Berlin,OU=IT,O=Musterfirma,C=
aka: <online@klaussner.biz>
sha2_fpr: F7:9C:E5:0B:EB:01:36:A8:8D:39:05:FF:AF:57:63:A0:72:72:4B:B5:55:E
sha1_fpr: 53:7C:25:E1:56:7A:C0:19:33:3A:82:F7:29:36:B4:6F:B6:6F:DA:C0
md5_fpr: E2:F6:77:95:12:93:EA:8E:04:58:B4:5E:69:EF:D7:9E
certid: 770A434B05FFB037EEFB758CEDB0D56EC840F6C3.08382729464162
keygrip: 080B9ECDF57471463AB04D8E00375921079AAC2E
notBefore: 2025-01-13 08:56:21
notAfter: 2026-01-12 23:00:00
hashAlgo: 1.2.840.10045.4.3.3
keyType: composite MLDSA6x5_ECDSA_P256
subjKeyId: 696A64AF62D5D9D4E601B89846D7DCBA7A3EC8B3
authKeyId: [none]
authKeyId.ki: 75C98D5480EDA42BA014A5D1570DD6B3F5A0D965
keyUsage: digitalSignature nonRepudiation keyEncipherment keyAgreement
extKeyUsage: [none]
policies: [none]
chainLength: not a CA
crlDP: [none]
authInfo: [none]
subjInfo: [none]
Aktualisieren
No changes in user experience


test - Message (HTML)
File
Message
Insert
Options
Format Text
Review
Help
Tell me what you want to do
Paste
Cut
Copy
Format Painter
Clipboard
Basic Text
Address Book
Check Names
Names
Attach File
Attach Item
Signature
Include
Follow Up
High Importance
Low Importance
Tags
Secure
Sign
Encrypt
Send
To...
qu-gov.test@mail.tn.mes
Cc...
Subject
test
Test123
Implementation overrides S/MIME from Outlook with dedicated button
File
Home
Send / Receive
Folder
View
Help
Tell me what you want to do
Change View
Reset View
Show as Conversations
Conversation Settings
Message Preview
Date
From
Size
Subject
Arrange
Search Current Mailbox
All
Unread
From
Subject
Yesterday
online@klaussner.biz
test enc
enc <end>
Inbox
Entwürfe
Gesendet
Papierkorb 1
Archiv
Outbox
Spam
Search Folders
test enc
online@klaussner.biz
To pqc@klaussner.biz
GpgOL: Level 3 trust in 'online@klaussner.biz'
enc

bundesdruckerei.

PQC Certificate Management System



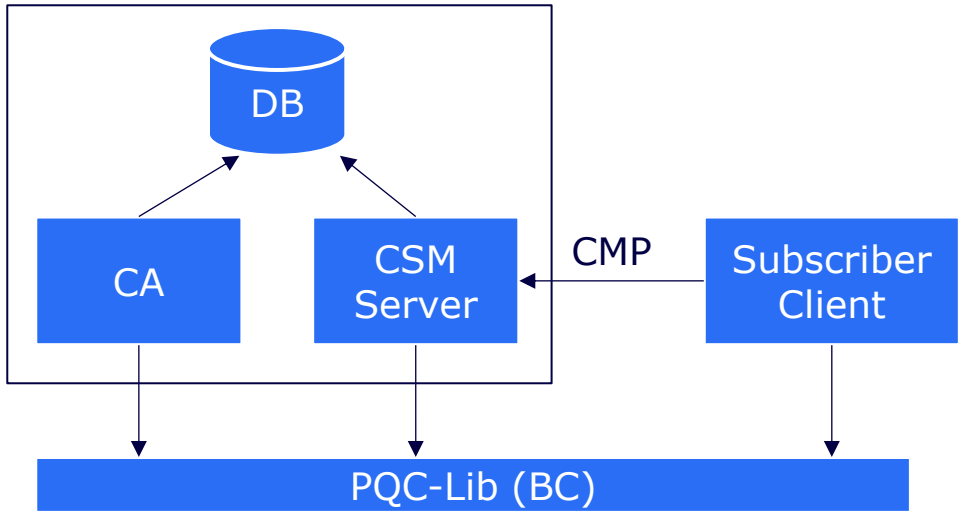
PQC Certificate Management System

Cryptographic Schemes

- ECDH, RSA encryption
- ML-KEM (Kyber, NIST Draft FIPS 203)
- ECDSA, RSA signature
- ML-DSA (Dilithium, NIST Draft FIPS 204)
- SLH-DSA (Sphincs+, NIST Draft FIPS 205)
- LMS, XMSS (NIST SP 800-208)

Plain/Hybrid/Mixed PKIs

- Composite Signatures/KEMs (IETF Drafts)
- Intelligent Composed Algorithms (AND, OR, K-of-N)
- Certificate issuance via Certificate Management Protocol
- Revocation: Certificate Revocation List



PQC Subscriber Client

Presets of Root/SubCA combinations, e.g.

- LMS -> ML-DSA+ECDSA
- ML-DSA+ECDSA -> ML-DSA+ECDSA
- SLH-DSA -> SLH-DAS
- …many more

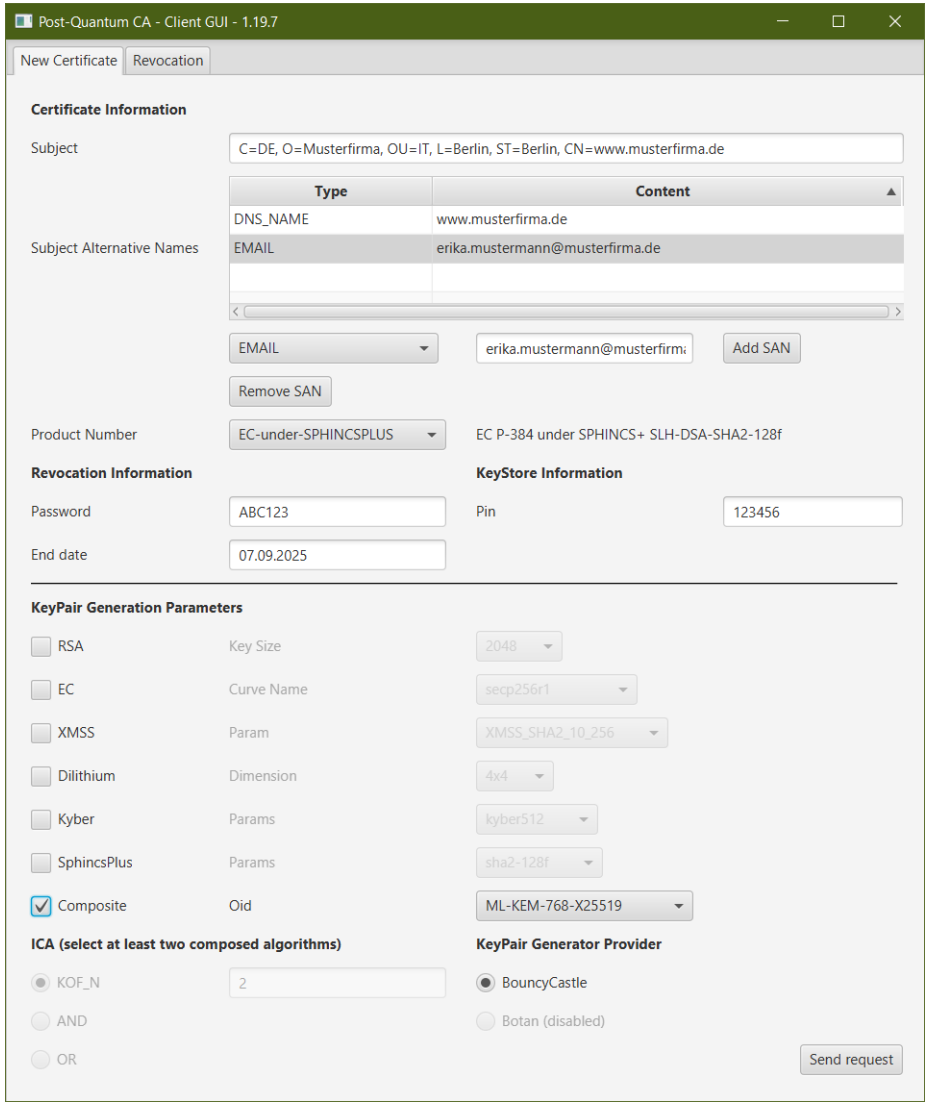
Open Topics

- Proof of possession
- HSM support

X.509 stuff

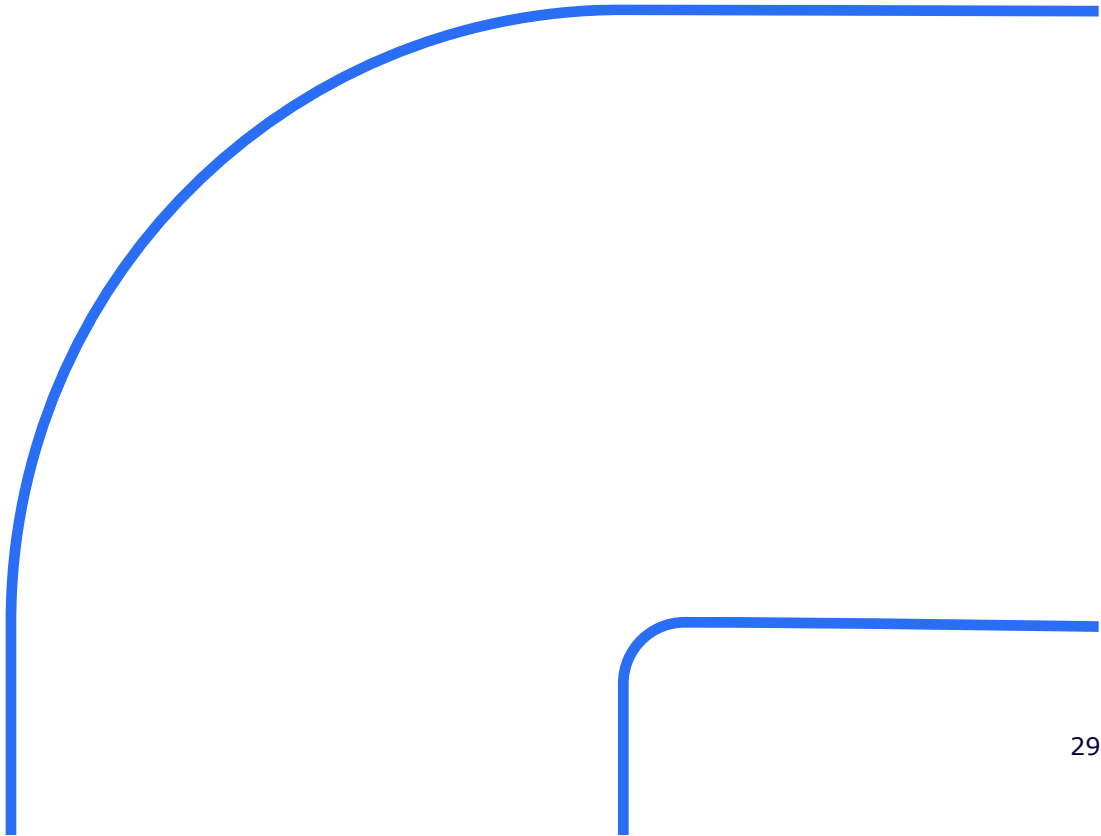
Select Root/SubCA

Select your algorithm



Yet to Solve

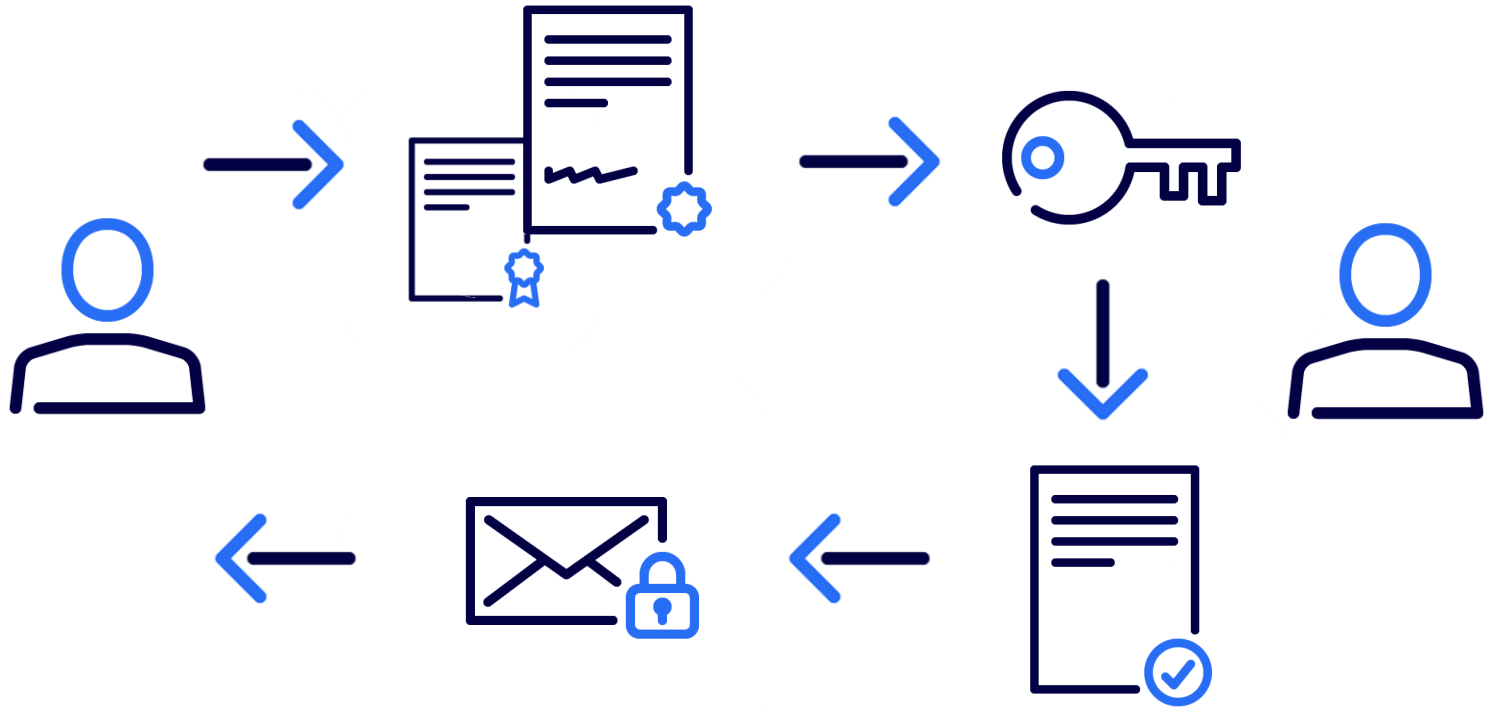
Automatic Distribution of Encryption Key



Automatic Distribution of Encryption Key

Today

1. user A sends signed mail with **one** Certificate
2. User B can extract A’s public key from its certificate and verify the signed mail
3. User B can use A’s public key to encrypt a mail and sends it back
4. User A can decrypt B’s mail

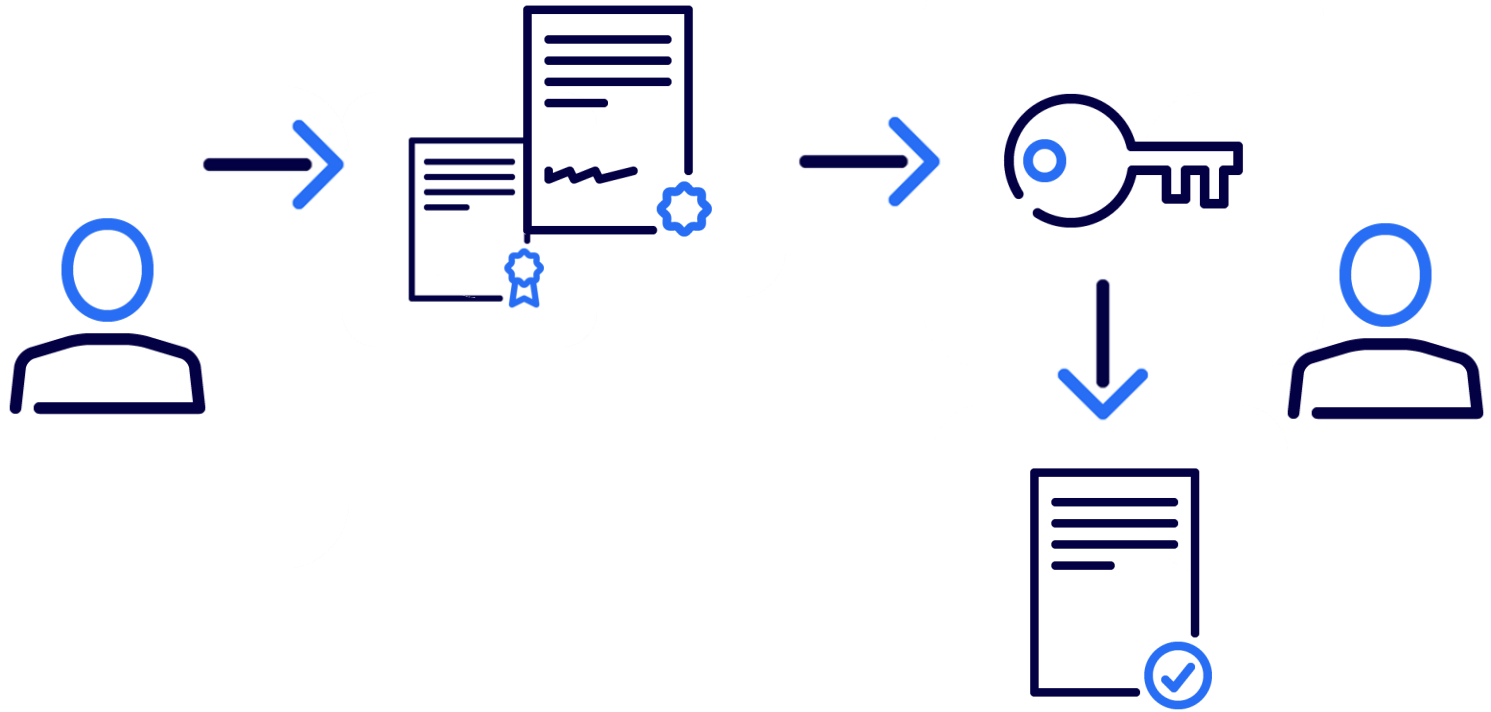


Automatic Distribution of Encryption Key

With PQC

PQC algorithms can not both sign and encrypt

- only signature certificate can be distributed
- separate encryption certificate is needed
- manual distribution is cumbersome

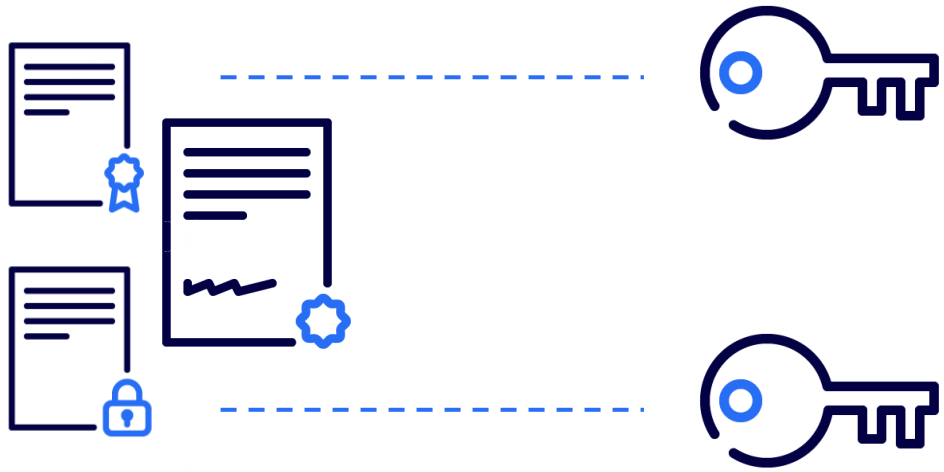


Automatic Distribution of Encryption Key

Solution 1 – Application Layer:

Send two certificates

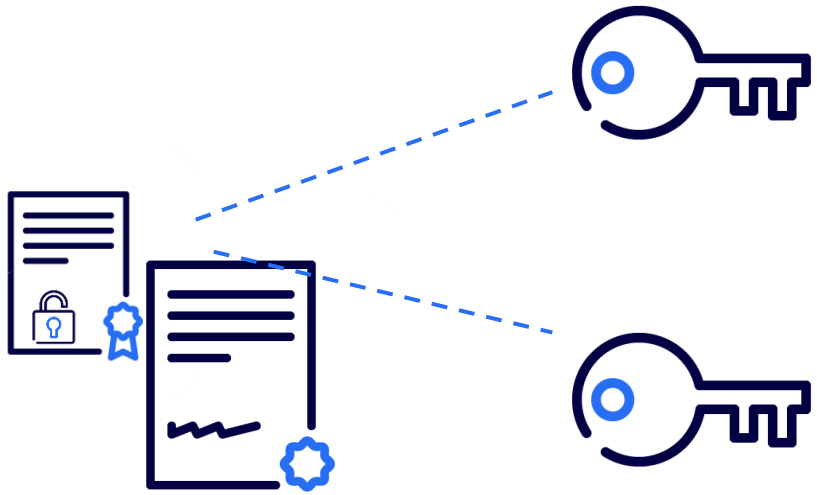
- support by each application needed
- experience shows its prone to errors



Automatic Distribution of Encryption Key

Solution 2 – Protocol Layer

ISARA Catalyst



- ✓ one certificate
- ✓ specified (although not intended this way)
- ✓ usable with ICA and Composite keys

- – needs adapter code to separate keys

Automatic Distribution of Encryption Key

Solution 3 – Crypto Layer:

Extension for Intelligent Composed Algorithms

- ✓ one compound key combining signature key(s) and encryption key(s)
- ✓ one certificate

– specification required

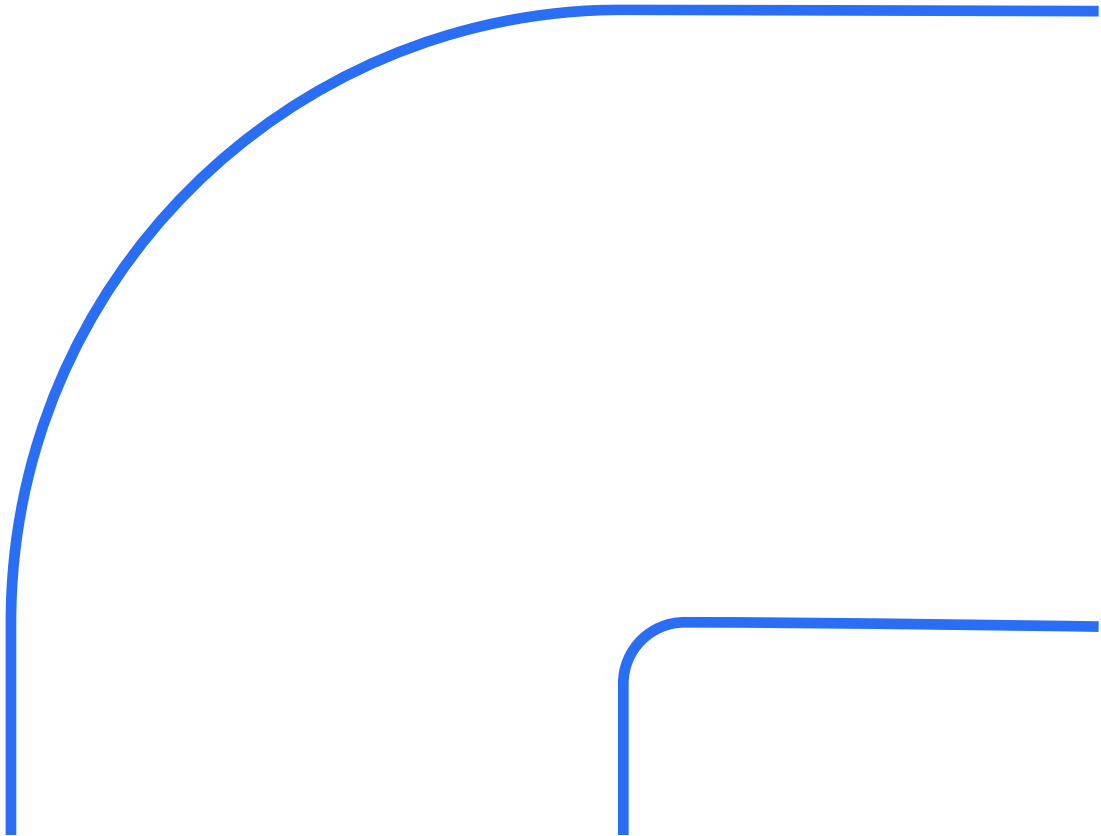
bundesdruckerei.

Hybrid PQC E-Mail Prototype

- ✓ Hybrids on crypto level are easy to integrate
- ✓ user experience remains simple

t.b.d.

- ○ automatic encryption key distribution



Thank you.

Jan Klaussner

Bundesdruckerei GmbH
Innovations
email: jan.klaussner@bdr.de
Phone: + 49 (0) 151 – 56001986

Part of the Bundesdruckerei Group