# KEM Certificate Signing Request Protocol and Key Exchange Protocol

Speakers:

Austin B. Y. Lin (Chunghwa Telecom Laboratories)

John Gray (Entrust)

Abel C. H. Chen (Chunghwa Telecom Laboratories)

# Outline

Introduction

Related Work

KEM Certificate Signing Request Protocol

Discussions on Dual-usage DSA-KEM Certificate Formats

Key Exchange Protocol

Demo

# Introduction

The current Certificate Signing Request (CSR) protocol does not support Proof of Possession (PoP) for PQC KEM (Key Encapsulation Mechanism) certificates.

Therefore, this talk proposes a KEM CSR protocol for the application of KEM certificates.

Additionally, some potential scenarios, such as **V2X (Vehicle-to-Everything) communications**, **use dual-usage certificates** that support both digital signatures and data encipherment.

Therefore, this talk also presents potential schemes for dual-usage certificates and comparison of their pros and cons with traditional pure certificates.

# Introduction

We will focus on the following topics:

- KEM Certificate Signing Request Protocol to solve KEM POP issue
- Discussions on Dual-usage DSA-KEM Certificate Formats
- Key Exchange Protocol

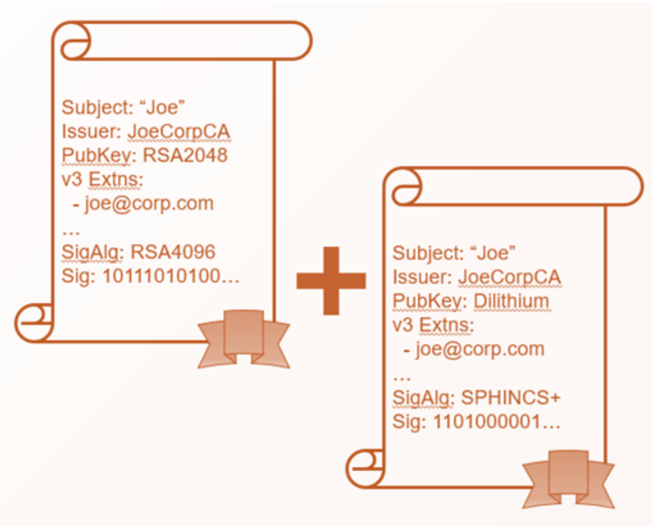
# Related Work

Hybrid Certificates:

Composite, Catalyst and Chameleon

# Options for Dual mode X.509 Certificates

## Multi-cert

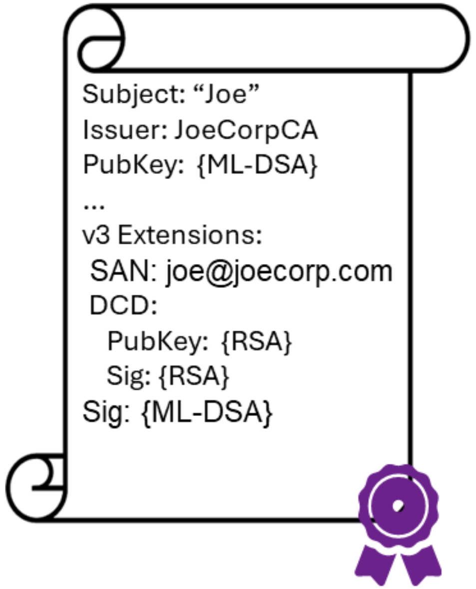



## "Hybrid" Catalyst™ [1]

IETF: draft-truskovsky-lamps-pq-hybrid-x509

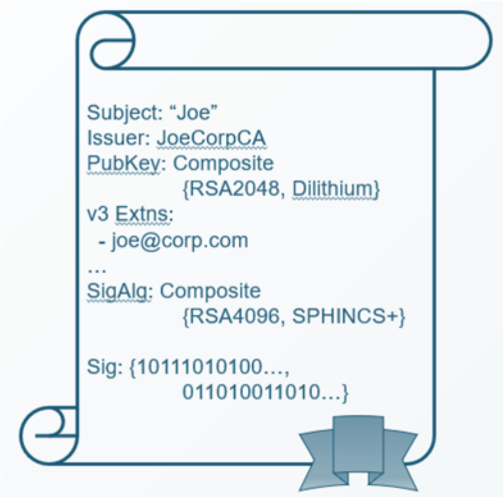

## CHAMELEON[2]

IETF: draft-bonnell-lamps-chameleon-certs



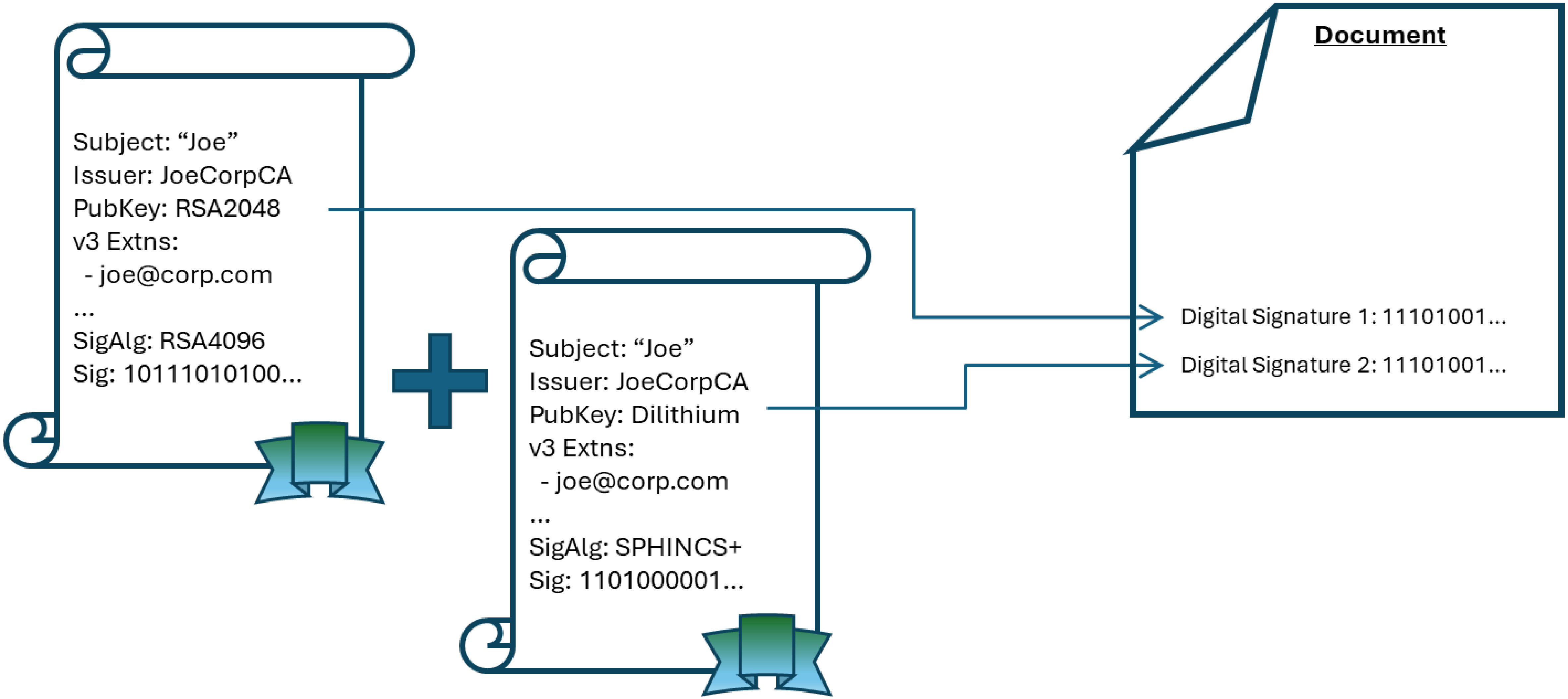

## Composite [3]

IETF: draft-ietf-lamps-pq-composite-sigs
draft-ietf-lamps-pq-composite-kem

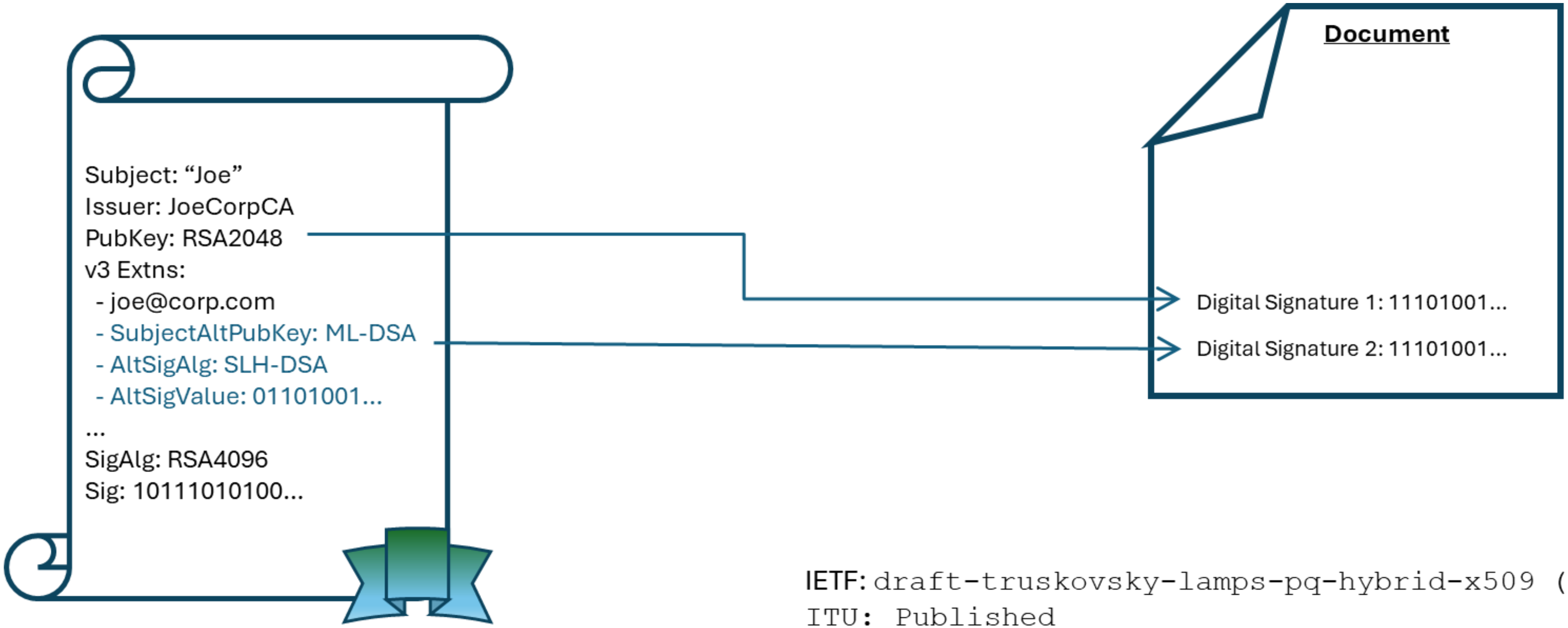



[1] ISARA - Entrust - Cisco collaboration; IETF and ISO drafts
[2] Entrust – Digicert – KeyFactor collaboration; IETF draft
[3] Entrust – CableLabs – Cisco collaboration; IETF draft

# Multi Certificate Approaches (Nothing New here)



# Hybrid Catalyst Certificate Format




IETF: `draft-truskovsky-lamps-pq-hybrid-x509 (rejected)`
`ITU: Published`

# Chameleon Certificates

| TRADITIONAL CERTIFICATE |
| --- |
| Subject: cn=joe |
| Issuer: CACorp |
| Serial: 07 |
| SPKI: { alg: RSA<br>key:8eff38e8... } |
| Extensions: |
| SANs: joe.com |
| Sig: {RSA} |

diff

diff

| PQ CERTIFICATE |
| --- |
| Subject: cn=joe |
| Issuer: CACorp |
| Serial: 08 |
| SPKI: { alg: ML-DSA-65<br>key:79eb4a2... } |
| Extensions: |
| SANs: joe.com |
| Sig: {ML-DSA-65} |

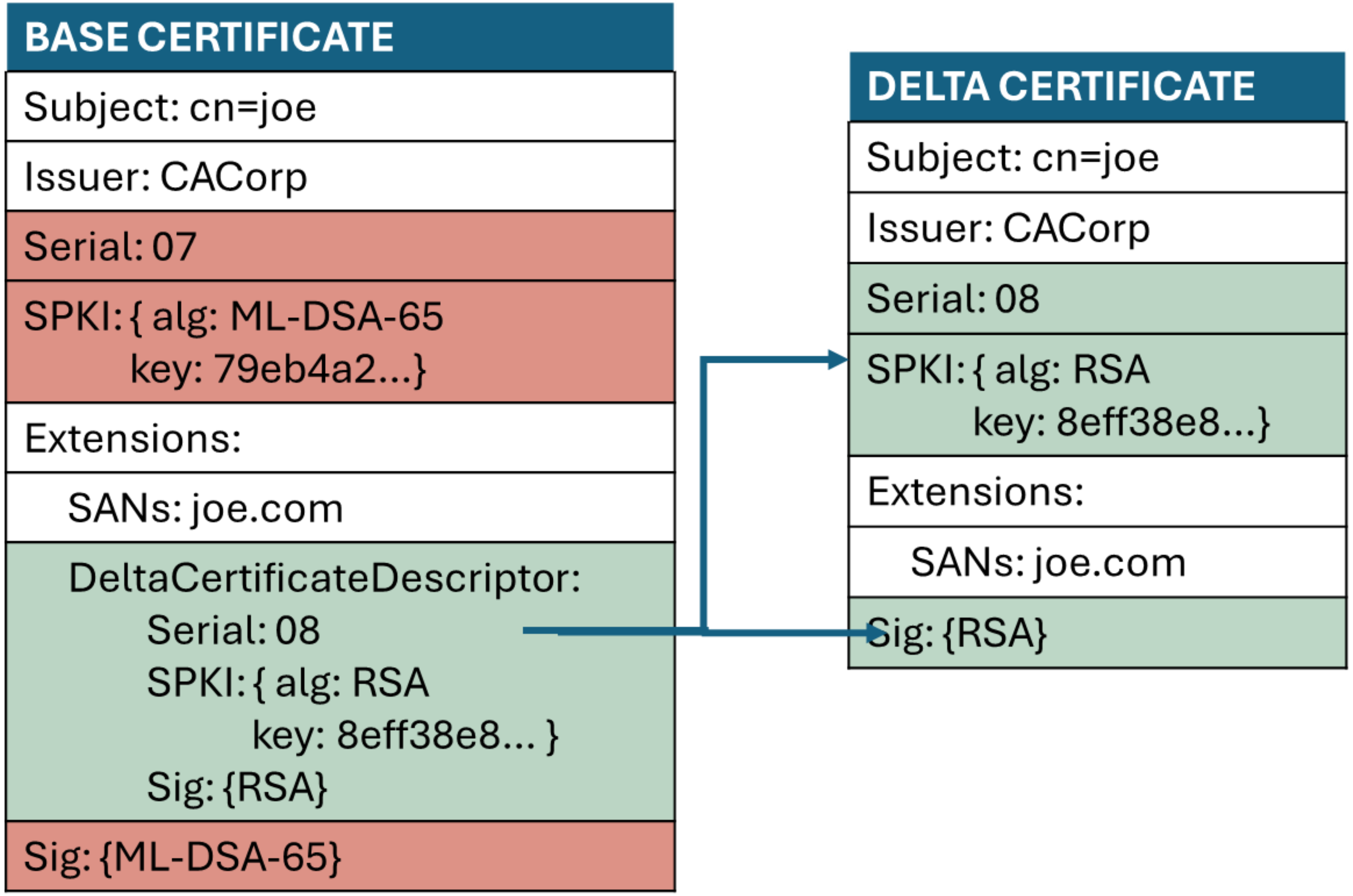
Core Idea – Naïve Parallel Certificates

# Chameleon

A 2023 re-do of Catalyst.

DeltaCertificateDescriptor is a v3 extension that allows you to encode the differences between two parallel certificates.

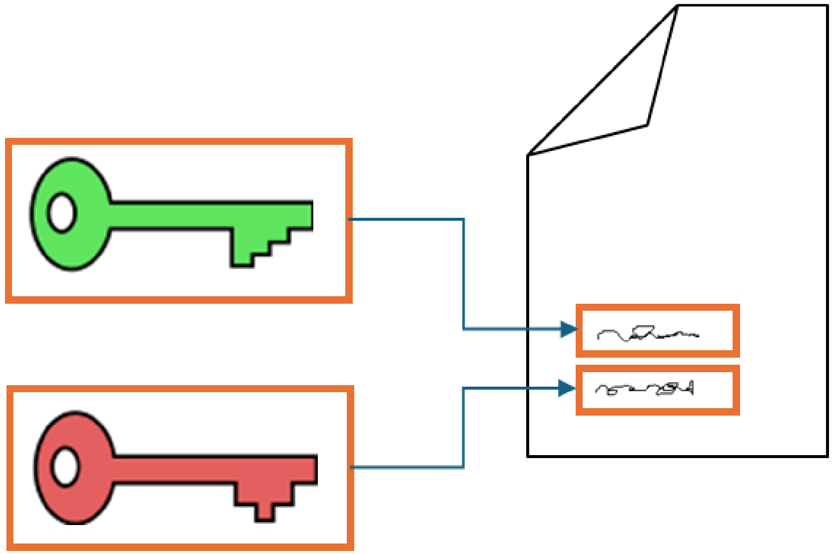
Basically, you can “bury” one cert inside another and easily
“extract” the inner cert.



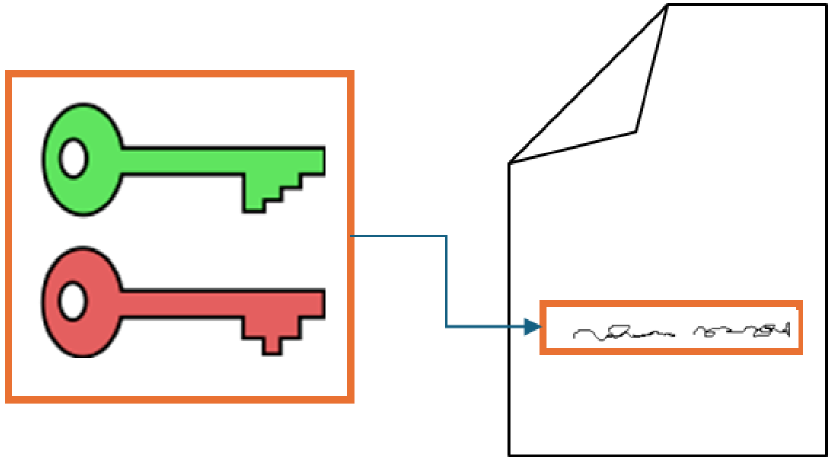

https://datatracker.ietf.org/doc/draft-bonnell-lamps-chameleon-certs/

# Composite Keys and Signatures

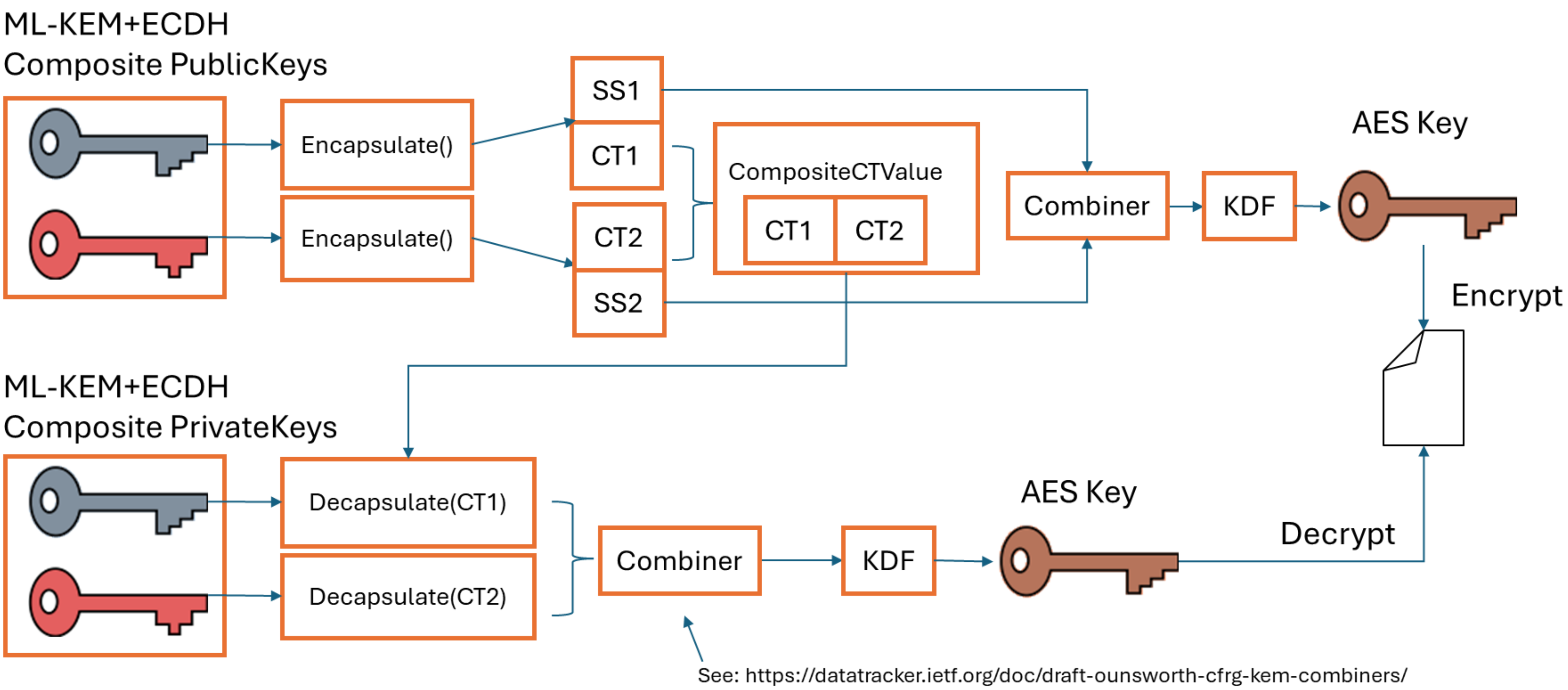
(1) Independent keys and signature objects



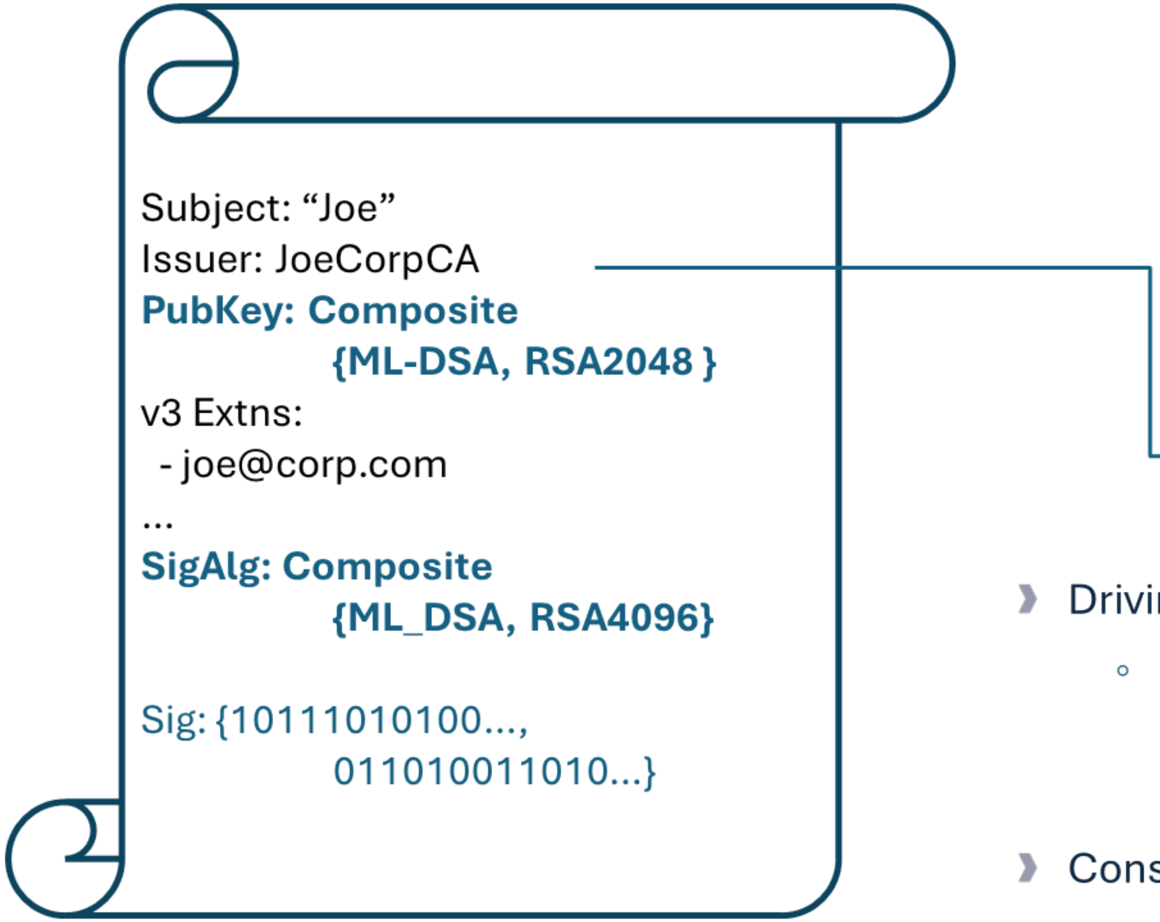
(2) Combined key and signature object

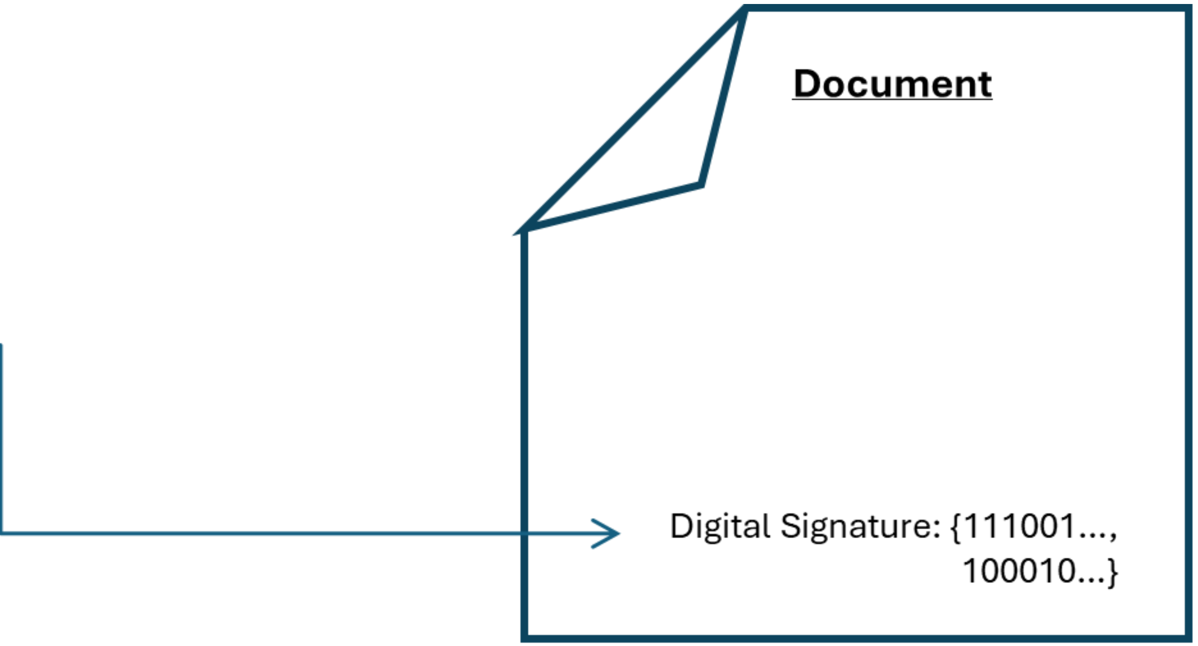


# Composite KEM



# Composite ML-DSA Certificates




- Driving motivation:
  - “Drops into any existing PubKey / Sig field; no modification needed to X.509 or the document format, other than the new OIDs for Composite structs.”
- Cons:
  - Backwards compatibility is tricky.

# Hybrid Certificate Summary

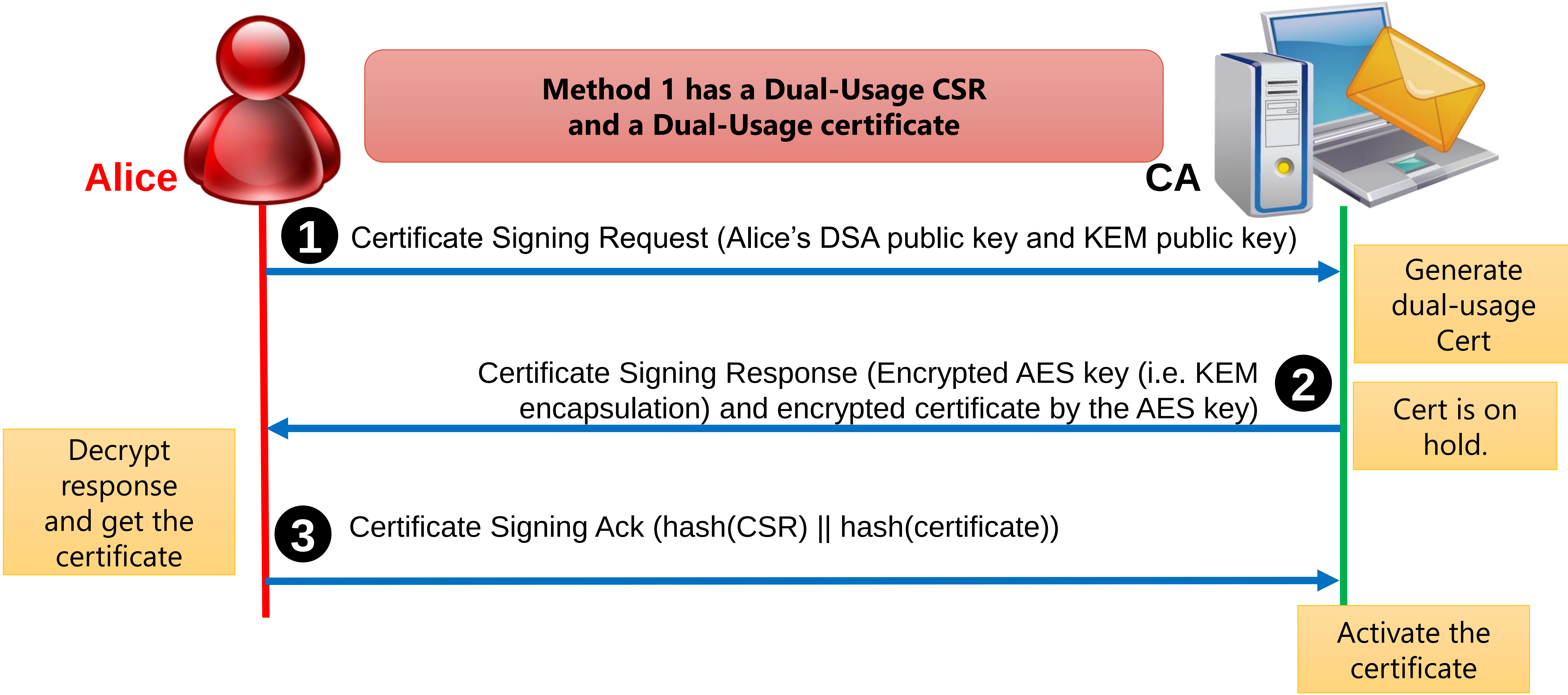
| | Multi-cert | Chameleon | Hybrid | Composite |
|---|---|---|---|---|
| (P + Q) Non-separability | No | Nested | Nested | Strong |
| Backwards-compatible with "legacy" x509 infrastructure | Yes (for Legacy)<br>No (For PQ) | Yes (Binary) | Yes (Binary) | No |
| Protocol Compatibility (TLS, IPSec, S/MIME, code signing, etc) | No | No | No | Yes |
| Strong P+Q Security | No | No | No | Yes |
| Forward PQ Migration Capable | Yes | Yes | No | Partial |
| Intellectual Property Rights Claims | None | None | ISARA Opened in 2022 | CableLabs Open Patent |
| General Public support | Some | New (IETF 117) | IETF rejected | Yes |
| Standards maturity | Favoured by some IETF members | New | ITU | Adopted at IETF |

# KEM Certificate Signing Request Protocol

Authors:

Abel C. H. Chen, Mike Ounsworth, James W. H. Tung, John Gray, and Austin B. Y. Lin

# KEM CSR Protocol (Method 1)



# KEM CSR Protocol (Method 1)

Alice sends a **Dual-Usage CSR** based on PKCS#10 to RA or CA.

CA issues a **Dual-Usage certificate** and send an **enveloped data** with the encrypted certificate based on PCKS#7 to Alice.

| **Dual-Usage CSR(PKCS#10)** |
|---|
| Subject: cn=Alice |
| SPKI: {alg: ML-DSA-65<br>key: ...} |
| Extensions: |
| **KEM-SPKI**: {alg: ML-KEM-768<br>key: ...} |
| Sig: {ML-DSA-65} |

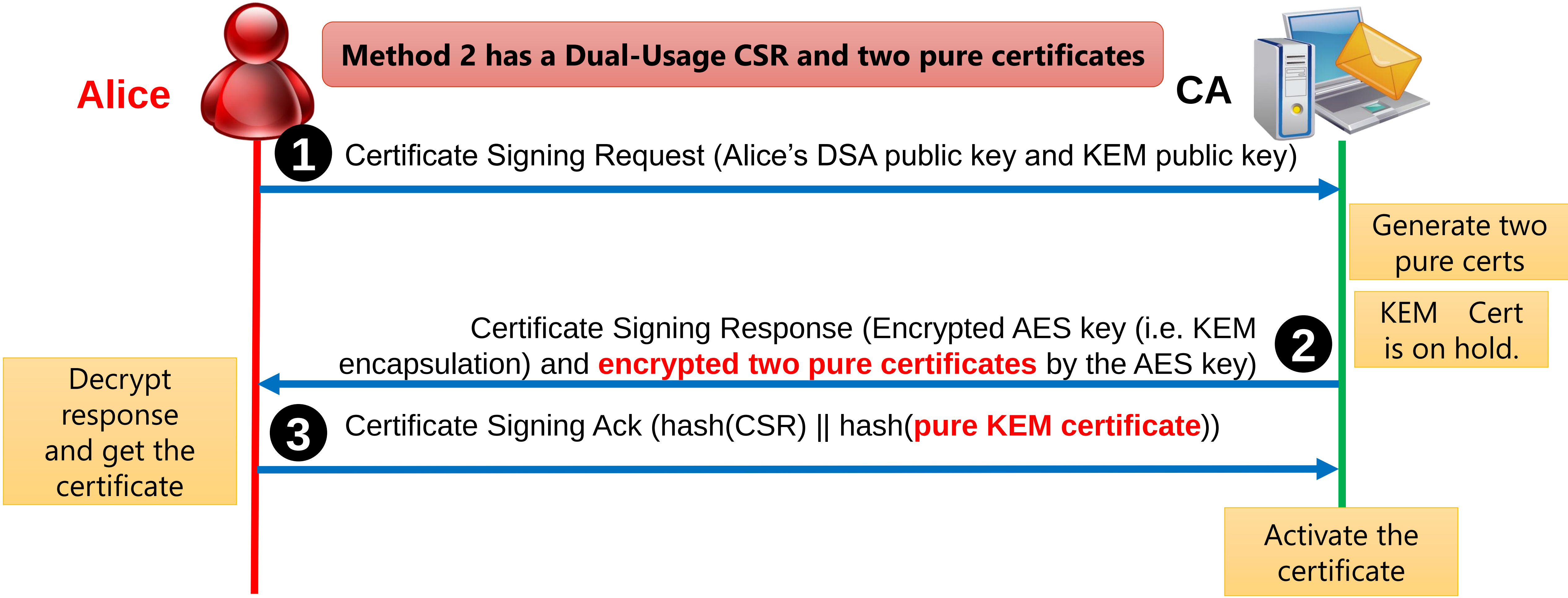
Need to be standardized

| **EnvelopedData (PKCS#7)** |
|---|
| RecipientInfos:<br>KEMRecipientInfo: {<br>rid: ...<br>**kem: ML-KEM-768**<br>**kemct: ML-KEM Encapsulation**<br>kdf: KMAC256-KDF<br>wrap: aes256-wrap<br>encryptedKey: ...} |
| EncryptedContentInfo: {<br>ContentEncryptionAlgorithmIdentifier: AES-256-CBC<br>EncryptedContent: **encrypted dual-usage certificate** |

RFC 9629

# KEM CSR Protocol (Method 2)

Response an encrypted Zip file including a pure DSA-based certificate and a pure KEM-based certificate



# KEM CSR Protocol (Method 2)

Alice sends a <u>**Dual-Usage CSR**</u> based on PKCS#10 to RA or CA.

CA issues <u>**two pure certificates**</u> and send an <u>**enveloped data**</u> with the encrypted certificate based on PCKS#7 to Alice.

| **Dual-Usage CSR** |
|---|
| Subject: cn=Alice |
| SPKI: {alg: ML-DSA-65<br>key: ...} |
| Extensions: |
| **KEM-SPKI**: {alg: ML-KEM-768<br>key: ...} |
| Sig: {ML-DSA-65} |

Need to be standardized

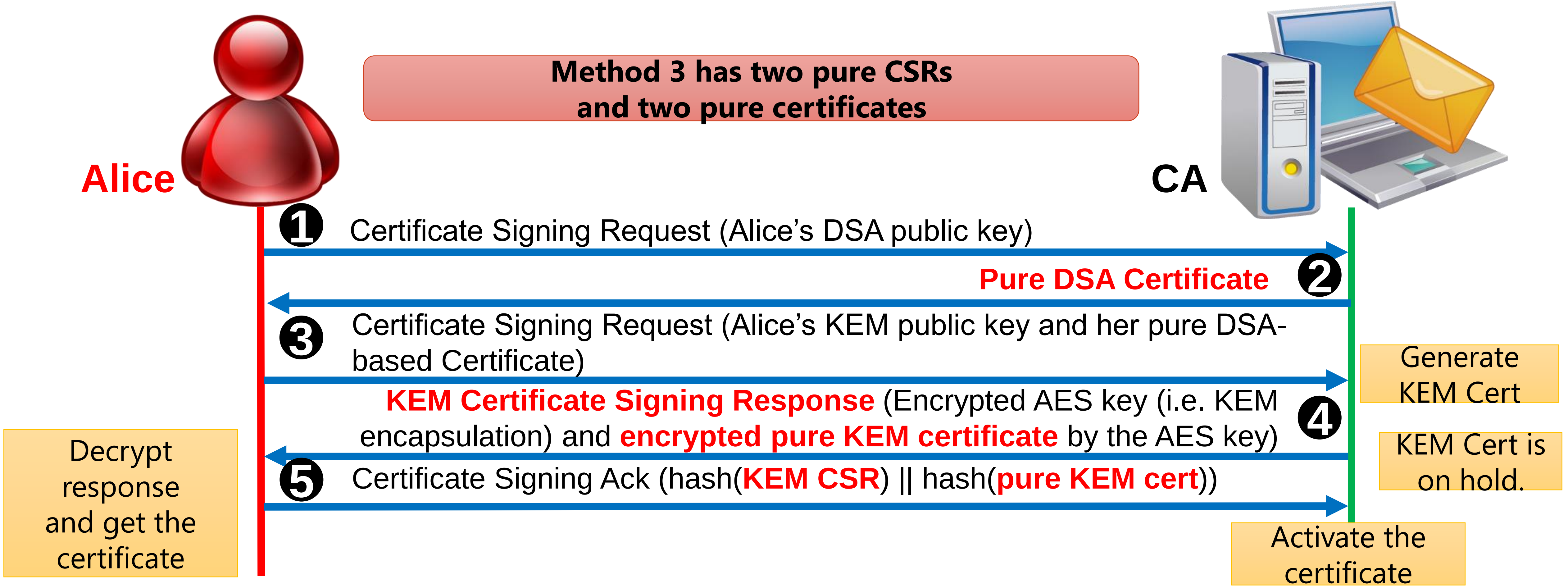
| **EnvelopedData (PKCS#7)** |
|---|
| RecipientInfos:<br>KEMRecipientInfo: {<br>rid: ...<br>**kem: ML-KEM-768**<br>**kemct: ML-KEM Encapsulation**<br>kdf: KMAC256-KDF<br>wrap: aes256-wrap<br>encryptedKey: ...} |
| EncryptedContentInfo: {<br>ContentEncryptionAlgorithmIdentifier: AES-256-CBC<br>EncryptedContent: <u>**encrypted two pure certificates**</u>} |

RFC 9629

# KEM CSR Protocol (Method 3)

Apply pure DSA certificate using Pure DSA CSR

Apply pure KEM certificate using  CSR contains  newly issued DSA certificate



# KEM CSR Protocol (Method 3)

Alice sends a **pure DSA CSR** based on PKCS#10 to RA or CA.

Alice sends a **pure KEM CSR** with the pure DSA certificate to RA or CA.

| KEM Certificate Signing Request (PKCS#10) |
|---|
| Subject: cn=Alice |
| SPKI: {alg: ML-KEM-768<br>key: ...} |
| Extensions: |
| **DSA-Cert**: the pure DSA certificate |
| Sig: {ML-DSA-65} |

Need to be standardized

| EnvelopedData (PKCS#7) |
|---|
| RecipientInfos:<br>KEMRecipientInfo: {<br>rid: ...<br>**kem: ML-KEM-768**<br>**kemct: ML-KEM Encapsulation**<br>kdf: KMAC256-KDF<br>wrap: aes256-wrap<br>encryptedKey: ...} |
| EncryptedContentInfo: {<br>ContentEncryptionAlgorithmIdentifier: AES-256-CBC<br>EncryptedContent: **encrypted KEM certificate**} |

RFC 9629

# Experimental Results of Method 3

**Message Lengths Based on two CSRs and two certificates (Unit: Bytes)**

| Message | Security Level 1 (ML-DSA-44, ML-KEM-512) | Security Level 3 (ML-DSA-65, ML-KEM-768) | Security Level 5 (ML-DSA-87, ML-KEM-1024) |
|---|---|---|---|
| Pure DSA Certificate Signing Request | 3,820 | 5,349 | 7,307 |
| Response (Pure DSA Certificate) | 3,959 | 5,488 | 7,446 |
| Pure KEM Certificate Signing Request | 7,287 | 10,089 | 13,749 |
| KEM Certificate Signing Response (Encrypted Cert.) | 4,422 | 6,038 | 8,214 |
| Total Lengths of Requests | 11,107 | 15,438 | 21,056 |
| Total Lengths of Responses | 8,381 | 11,526 | 15,660 |

Include a pure DSA cert

# Comparison Results

| Message | Security Level 1 (ML-DSA-44, ML-KEM-512) | Security Level 3 (ML-DSA-65, ML-KEM-768) | Security Level 5 (ML-DSA-87, ML-KEM-1024) |
|---|---|---|---|
| Request (Method 1 and Method 2) | 4,657 | 6,570 | 8,912 |
| Request (Compared Method 3) | 11,107 | 15,438 | 21,056 |
| Response (Method 1) with Composite Scheme | 5,750 | 8,006 | 10,822 |
| Response (Method 1) with Catalyst Scheme | 5,782 | 8,022 | 10,854 |
| Response (Method 1) with Chameleon Scheme | 8,246 | 11,382 | 15,526 |
| Response (Compared Method 2) | 8,614 | 11,750 | 15,862 |
| Response (Compared Method 3) | 8,381 | 11,526 | 15,660 |

Dual-usage CSR

Toal length of two CSRs

Include Dual-usage Cert in The response

Total length of two Certs

Total length of two Responses

# Discussions on Dual-usage Certificate Formats

Authors:

Abel C. H. Chen, Mike Ounsworth, James W. H. Tung, John Gray, and Austin B. Y. Lin

# Pure DSA and KEM Certificates

| Pure Certificate (X.509) |
|---|
| Subject: cn=Alice |
| SPKI: { **alg: ML-DSA-65** key: **ML-DSA-65 key** } |
| Extensions: |
| Key Usage: {digitalSignature} |
| Sig: {ML-DSA-87} |

Pure DSA-based Certificate

| Pure Certificate (X.509) |
|---|
| Subject: cn=Alice |
| SPKI: { **alg: ML-KEM-768** key: **ML-KEM-768 key** } |
| Extensions: |
| Key Usage: {dataEncipherment} |
| Sig: {ML-DSA-87} |

Pure KEM-based Certificate

# DSA-KEM Dual-Usage Certificate Format

## Daul-Usage Certificate (X.509)

Subject: cn=Alice

Need to be standardized

SPKI: {
  **alg: ML-DSA-65||ML-KEM-768**
  key: {
    ML-DSA-65 key ||
    **ML-KEM-768 key**
  }
}

Extensions:

Key Usage: {
  digitalSignature
  dataEncipherment}

Sig: {ML-DSA-87}

Composite

## Dual-Usage Certificate (X.509)

Subject: cn=Alice

SPKI: {
    alg: ML-DSA-65
    key: ...
}

Extensions:

Key Usage: {
  digitalSig
  dataEncipherment}

Need to be standardized

**KEM-SPKI**: {**alg: ML-KEM-768**
  **key: ...**}

Sig: {ML-DSA-87}

Catalyst

## Dual-Usage Certificate (X.509)

Subject: cn=Alice

SPKI: {
    {alg: ML-DSA-65
    key: ...}
  }

Extensions:

Key Usage: {digitalSignature}

DeltaCertificateDescriptor:

SPKI: { **alg: ML-KEM-768**
  **key: ...**}

Key Usage: {dataEncipherment}

Sig: {ML-DSA-87}

Sig: {ML-DSA-87}

Chameleon

# Comparison of Certificate Lengths (ML-DSA)

## Comparison of Certificate Lengths (Unit: Bytes)

| Certificate | Security Level 1 (ML-DSA-44, ML-KEM-512) | Security Level 3 (ML-DSA-65, ML-KEM-768) | Security Level 5 (ML-DSA-87, ML-KEM-1024) |
|---|---|---|---|
| Pure DSA | 3,959 | 5,488 | 7,446 |
| Pure KEM | 3,447 | 4,720 | 6,422 |
| Pure DSA + Pure KEM | 7,406 | 10,208 | 13,868 |
| Composite Scheme | 4,775 | 6,688 | 9,030 |
| Catalyst Scheme | 4,801 | 6,714 | 9,056 |
| Chameleon Scheme | 7,276 | 10,078 | 13,738 |

Reduce

Dual-usage Certificate

# Comparison of Certificate Lengths (SLH-DSA small-signature version)

## Comparison of Certificate Lengths (Unit: Bytes)

| Certificate | Security Level 1 (SLH-DSA-128s, ML-KEM-512) | Security Level 3 (SLH-DSA-192s, ML-KEM-768) | Security Level 5 (SLH-DSA-256s, ML-KEM-1024) |
|---|---|---|---|
| Pure DSA | 8,110 | 16,494 | 30,079 |
| Pure KEM | 8,883 | 17,635 | 31,587 |
| Pure DSA + Pure KEM | 16,993 | 34,129 | 61,666 |
| Composite Scheme | 8,929 | 17,697 | 31,665 |
| Catalyst Scheme | 8,953 | 17,721 | 31,689 |
| Chameleon Scheme | 16,864 | 34,000 | 61,536 |

**Reduce**

# Comparison of Certificate Lengths (SLH-DSA fast-signature)

## Comparison of Certificate Lengths (Unit: Bytes)

| Certificate | Security Level 1 (SLH-DSA-128f, ML-KEM-512) | Security Level 3 (SLH-DSA-192f, ML-KEM-768) | Security Level 5 (SLH-DSA-256f, ML-KEM-1024) |
|---|---|---|---|
| Pure DSA | 17,342 | 35,934 | 50,143 |
| Pure KEM | 18,115 | 37,075 | 51,651 |
| Pure DSA + Pure KEM | 35,457 | 73,009 | 101,794 |
| Composite Scheme | 18,161 | 37,137 | 51,729 |
| Catalyst Scheme | 18,185 | 37,161 | 51,753 |
| Chameleon Scheme | 35,328 | 72,881 | 101,665 |

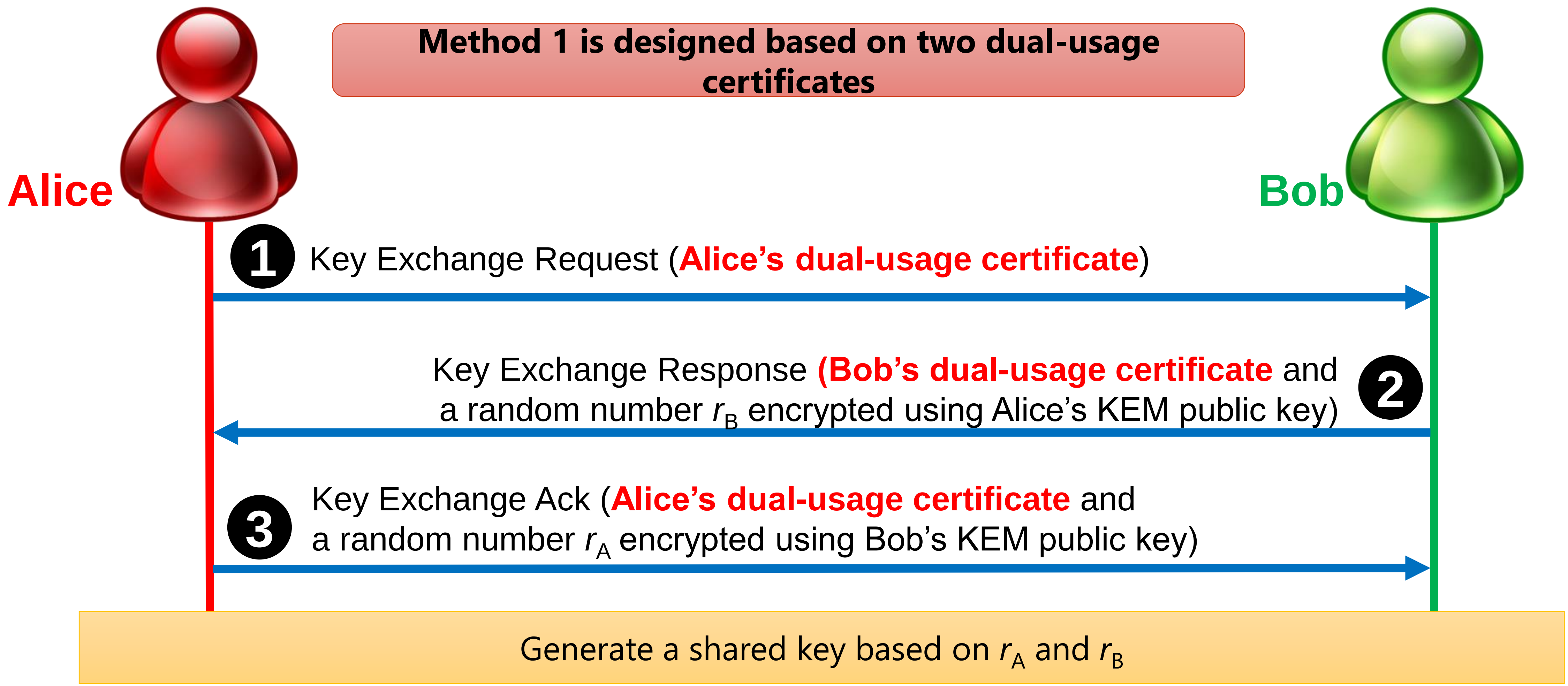
Reduce

# Key Exchange Protocol and Application

Authors:

Abel C. H. Chen, James W. H. Tung, Austin B. Y. Lin,
Chin-Ling Chen, Ching-Chun Chang, and Chin-Chen Chang

# Key Exchange Protocol (Method 1)



# Key Exchange Protocol (Method 2)

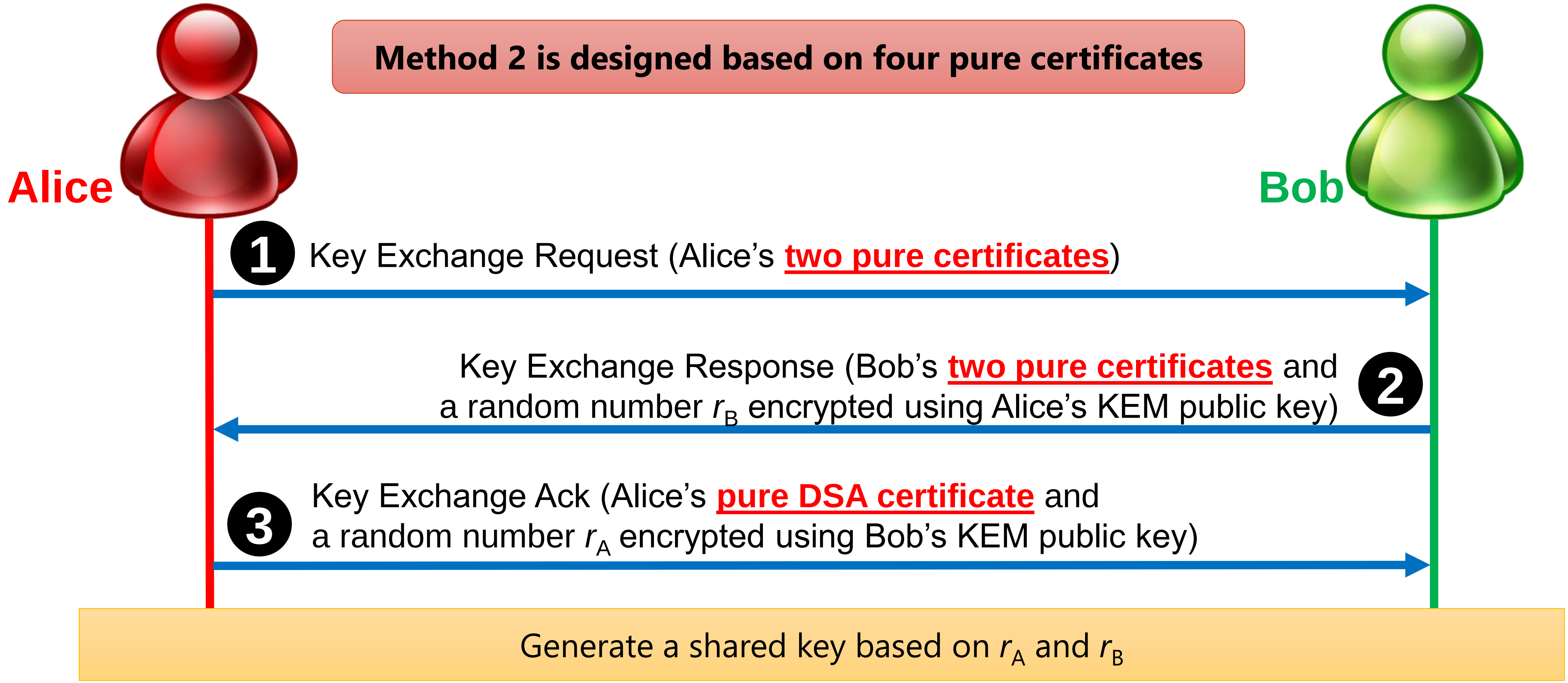
Bob sends signed data with a **random number $r_B$**, encrypted using Alice's KEM public key (i.e. the encapsulation), to Alice.

Alice sends signed data with a **random number $r_A$**, encrypted using Bob's KEM public key (i.e. the encapsulation), to Bob.

Then, **the shared key can be generated using $r_A$ and $r_B$**.

| **SignedData (PKCS#7) (from Bob)** |
|---|
| DigestAlgorithmIdentifiers: SHAKE-256 |
| ContentInfo: {<br>  **messageType: kepResp**<br>  **message: ML-KEM Encapsulation (using Alice's public key)**}<br>Need to be standardized |
| ExtendedCertificatesAndCertificates: {<br>  CA's certificate<br>  Bob's certificate} |
| SignerInfos: {<br>  SignerInfo: {<br>    Serial: ...<br>    DigestAlgorithmIdentifier: SHAKE-256<br>    SignedAttributes: {<br>      signingTime: ...<br>      messageDigest: ...}<br>    SignatureAlgorithmIdentifier: **ML-DSA-65 (Bob)**<br>    SignatureValue: **ML-DSA-65 (Bob)** }<br>} |

# Key Exchange Protocol (Method 2)



# Comparison of Key Exchange Request

## Comparison of Message Lengths (Unit: Bytes)

| Method | Security Level 1 (ML-DSA-44, ML-KEM-512) | Security Level 3 (ML-DSA-65, ML-KEM-768) | Security Level 5 (ML-DSA-87, ML-KEM-1024) |
|---|---|---|---|
| Method 1 with Composite Scheme | 7,549 | 10,351 | 14,011 |
| Method 1 with Catalyst Scheme | 7,575 | 10,377 | 14,037 |
| Method 1 with Chameleon Scheme | 10,050 | 13,741 | 18,719 |
| Method 2 | 10,180 (total length of two certs) | 13,871 (total length of two certs) | 18,849 (total length of two certs) |

# Comparison of Key Exchange Response

## Comparison of Message Lengths (Unit: Bytes)

| Method | Security Level 1 (ML-DSA-44, ML-KEM-512) | Security Level 3 (ML-DSA-65, ML-KEM-768) | Security Level 5 (ML-DSA-87, ML-KEM-1024) |
|---|---|---|---|
| Method 1 with Composite Scheme | 8,325 | 11,447 | 15,587 |
| Method 1 with Catalyst Scheme | 8,351 | 11,473 | 15,613 |
| Method 1 with Chameleon Scheme | 10,826 | 14,837 | 20,295 |
| Method 2 | 10,954 (total length of two certs) | 14,965 (total length of two certs) | 20,423 (total length of two certs) |

# Comparison of Key Exchange Ack

## Comparison of Message Lengths (Unit: Bytes)

| Method | Security Level 1 (ML-DSA-44, ML-KEM-512) | Security Level 3 (ML-DSA-65, ML-KEM-768) | Security Level 5 (ML-DSA-87, ML-KEM-1024) |
|---|---|---|---|
| Method 1 with Composite Scheme | 8,327 | 11,449 | 15,589 |
| Method 1 with Catalyst Scheme | 8,353 | 11,475 | 15,615 |
| Method 1 with Chameleon Scheme | 10,828 | 14,839 | 20,297 |
| Method 2 | 7,511(pure DSA) | 10,249(pure DSA) | 14,005(pure DSA) |

# Summary

## KEM Certificate Signing Request Protocol

- Support the **proof of possession** for KEM
- Support the request for a **dual-usage certificate**
- Support the request for two pure certificates (e.g., DSA and KEM)

## Key Exchange Protocol

- Support **bidirectional authentication**
- Support **key exchange based on KEM**

# Summary

## Pure DSA Certificate and Pure KEM Certificate

- A DSA public key and a KEM public key
- **Two** times the amount of information (e.g., common name , keyUsage)
- **Two** DSA signatures

## Dual-usage Certificate

- A DSA public key and a KEM public key
- **One** time the amount of information (e.g., common name, keyUsage)
- **One** DSA signature (<u>but two DSA signatures for chameleon</u>)

# Demo

# Thank you for your attention!

# Appendix

# Comparison of KEM-based Certificate Signing Request Protocol Based on SLH-DSA

# Experimental Results of Method 3

**Message Lengths Based on two CSRs and two certificates (Unit: Bytes)**

| Message | Security Level 1 (SLH-DSA-128s, ML-KEM-512) | Security Level 3 (SLH-DSA-192s, ML-KEM-768) | Security Level 5 (SLH-DSA-256s, ML-KEM-1024) |
|---|---|---|---|
| Pure DSA Certificate Signing Request | 7,970 | 16,354 | 29,938 |
| Response (Pure DSA Certificate) | 8,110 | 16,494 | 30,079 |
| Pure KEM Certificate Signing Request | 16,874 | 34,010 | 61,547 |
| KEM Certificate Signing Response (Encrypted Cert.) | 9,862 | 18,950 | 33,382 |
| Total Lengths of Requests | 24,844 | 50,364 | 91,485 |
| Total Lengths of Responses | 17,972 | 35,444 | 63,461 |

Include a pure DSA cert

# Comparison Results

## Comparison of Message Lengths (Unit: Bytes)

| Message | Security Level 1 (SLH-DSA-128s, ML-KEM-512) | Security Level 3 (SLH-DSA-192s, ML-KEM-768) | Security Level 5 (SLH-DSA-256s, ML-KEM-1024) |
|---|---|---|---|
| Request (Method 1 and Method 2) | 8,809 | 17,577 | 31,545 |
| Request (Compared Method 3) | 24,844 | 50,364 | 91,485 |
| Response (Method 1) with Composite Scheme | 9,910 | 19,014 | 33,462 |
| Response (Method 1) with Catalyst Scheme | 9,926 | 19,030 | 33,478 |
| Response (Method 1) with Chameleon Scheme | 17,846 | 35,318 | 63,334 |
| Response (Compared Method 2) | 18,198 | 35,670 | 63,686 |
| Response (Compared Method 3) | 17,972 | 35,444 | 63,461 |

# Experimental Results of Method 3

## Message Lengths Based on two CSRs and two certificates (Unit: Bytes)

| Message | Security Level 1 (SLH-DSA-128f, ML-KEM-512) | Security Level 3 (SLH-DSA-192f, ML-KEM-768) | Security Level 5 (SLH-DSA-256f, ML-KEM-1024) |
|---|---|---|---|
| Pure DSA Certificate Signing Request | 17,202 | 35,794 | 50,002 |
| Response (Pure DSA Certificate) | 17,342 | 35,934 | 50,143 |
| Pure KEM Certificate Signing Request | 35,338 | 72,891 | 101,676 |
| KEM Certificate Signing Response (Encrypted Cert.) | 19,094 | 38,390 | 53,446 |
| Total Lengths of Requests | 52,540 | 108,685 | 151,678 |
| Total Lengths of Responses | 36,436 | 74,324 | 103,589 |

Include a pure DSA cert

# Comparison Results

## Comparison of Message Lengths (Unit: Bytes)

| Message | Security Level 1 (SLH-DSA-128f, ML-KEM-512) | Security Level 3 (SLH-DSA-192f, ML-KEM-768) | Security Level 5 (SLH-DSA-256f, ML-KEM-1024) |
|---|---|---|---|
| Request (Method 1 and Method 2) | 18,041 | 37,017 | 51,609 |
| Request (Compared Method 3) | 52,540 | 108,685 | 151,678 |
| Response (Method 1) with Composite Scheme | 19,142 | 38,454 | 53,526 |
| Response (Method 1) with Catalyst Scheme | 19,158 | 38,470 | 53,542 |
| Response (Method 1) with Chameleon Scheme | 36,310 | 74,203 | 103,467 |
| Response (Compared Method 2) | 36,662 | 74,571 | 103,851 |
| Response (Compared Method 3) | 36,436 | 74,324 | 103,589 |

# Comparison of Key Exchange Protocol Based on SLH-DSA

# Comparison of Key Exchange Request

## Comparison of Message Lengths (Unit: Bytes)

| Method | Security Level 1 (SLH-DSA-128s, ML-KEM-512) | Security Level 3 (SLH-DSA-192s, ML-KEM-768) | Security Level 5 (SLH-DSA-256s, ML-KEM-1024) |
|---|---|---|---|
| Method 1 with Composite Scheme | 17,107 | 34,275 | 61,811 |
| Method 1 with Catalyst Scheme | 17,131 | 34,299 | 61,835 |
| Method 1 with Chameleon Scheme | 25,042 | 50,578 | 91,685 |
| Method 2 | 25,171 | 50,707 | 91,815 |

# Comparison of Key Exchange Response

## Comparison of Message Lengths (Unit: Bytes)

| Method | Security Level 1 (SLH-DSA-128s, ML-KEM-512) | Security Level 3 (SLH-DSA-192s, ML-KEM-768) | Security Level 5 (SLH-DSA-256s, ML-KEM-1024) |
| --- | --- | --- | --- |
| Method 1 with Composite Scheme | 17,883 | 35,371 | 63,387 |
| Method 1 with Catalyst Scheme | 17,907 | 35,395 | 63,411 |
| Method 1 with Chameleon Scheme | 25,818 | 51,674 | 93,261 |
| Method 2 | 25,945 | 51,801 | 93,389 |

# Comparison of Key Exchange Ack

Comparison of Message Lengths (Unit: Bytes)

| Method | Security Level 1 (SLH-DSA-128s, ML-KEM-512) | Security Level 3 (SLH-DSA-192s, ML-KEM-768) | Security Level 5 (SLH-DSA-256s, ML-KEM-1024) |
|---|---|---|---|
| Method 1 with Composite Scheme | 17,885 | 35,373 | 63,389 |
| Method 1 with Catalyst Scheme | 17,909 | 35,397 | 63,413 |
| Method 1 with Chameleon Scheme | 25,820 | 51,676 | 93,263 |
| Method 2 | 17,066 | 34,170 | 61,803 |

# Comparison of Key Exchange Request

Comparison of Message Lengths (Unit: Bytes)

| Method | Security Level 1 (SLH-DSA-128f, ML-KEM-512) | Security Level 3 (SLH-DSA-192f, ML-KEM-768) | Security Level 5 (SLH-DSA-256f, ML-KEM-1024) |
|---|---|---|---|
| Method 1 with Composite Scheme | 35,571 | 73,158 | 101,942 |
| Method 1 with Catalyst Scheme | 35,595 | 73,182 | 101,966 |
| Method 1 with Chameleon Scheme | 52,738 | 108,903 | 151,879 |
| Method 2 | 52,867 | 109,031 | 152,008 |

# Comparison of Key Exchange Response

## Comparison of Message Lengths (Unit: Bytes)

| Method | Security Level 1 (SLH-DSA-128f, ML-KEM-512) | Security Level 3 (SLH-DSA-192f, ML-KEM-768) | Security Level 5 (SLH-DSA-256f, ML-KEM-1024) |
|---|---|---|---|
| Method 1 with Composite Scheme | 36,347 | 74,254 | 103,518 |
| Method 1 with Catalyst Scheme | 36,371 | 74,278 | 103,542 |
| Method 1 with Chameleon Scheme | 53,514 | 109,999 | 153,455 |
| Method 2 | 53,641 | 110,125 | 153,582 |

# Comparison of Key Exchange Ack

## Comparison of Message Lengths (Unit: Bytes)

| Method | Security Level 1 (SLH-DSA-128f, ML-KEM-512) | Security Level 3 (SLH-DSA-192f, ML-KEM-768) | Security Level 5 (SLH-DSA-256f, ML-KEM-1024) |
|---|---|---|---|
| Method 1 with Composite Scheme | 36,349 | 74,256 | 103,520 |
| Method 1 with Catalyst Scheme | 36,373 | 74,280 | 103,544 |
| Method 1 with Chameleon Scheme | 53,516 | 110,001 | 153,457 |
| Method 2 | 35,530 | 73,053 | 101,934 |