
SCTE®
CABLE-TEC EXPO®
FAST FORWARD 2021
ATLANTA, GA
OCTOBER 11-14
SCTE
a subsidiary of CableLabs®
UNLEASH THE POWER OF LIMITLESS CONNECTIVITY
2021 Fall Technical Forum
SCTE® • NCTA • CABLELABS®

SCTE
a subsidiary of CableLabs

Security & Privacy

Enabling Encryption and Algorithm Revocation in Multi-Key Certificates

Massimiliano Pala

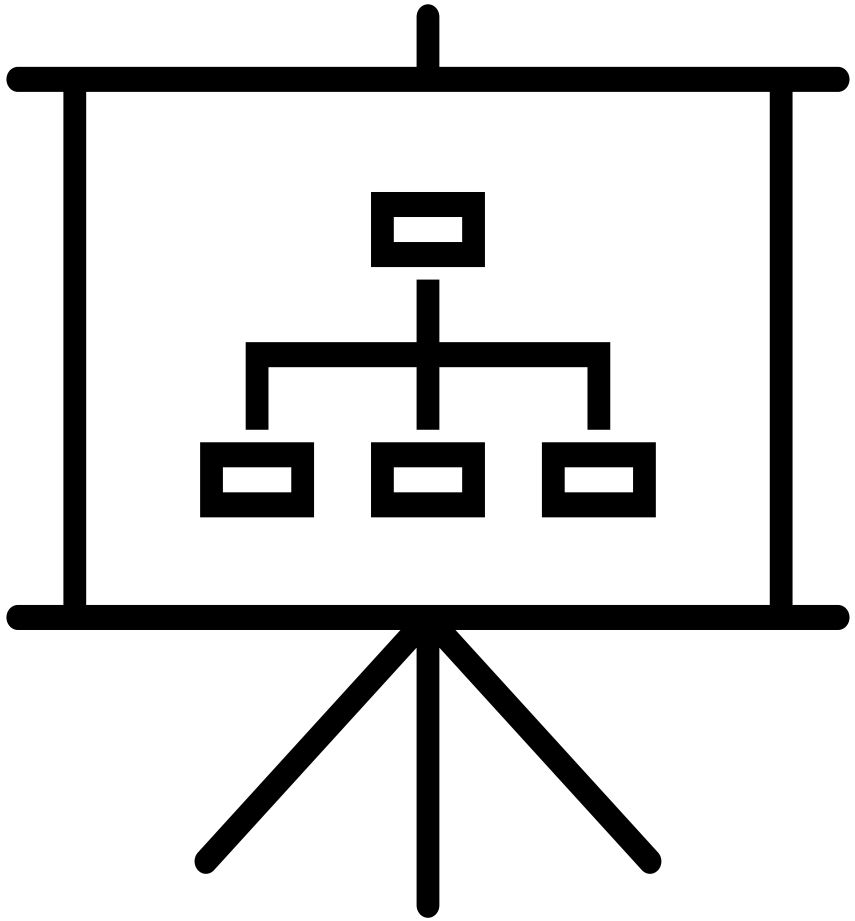
PKI Architectures Team, Director
CableLabs

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

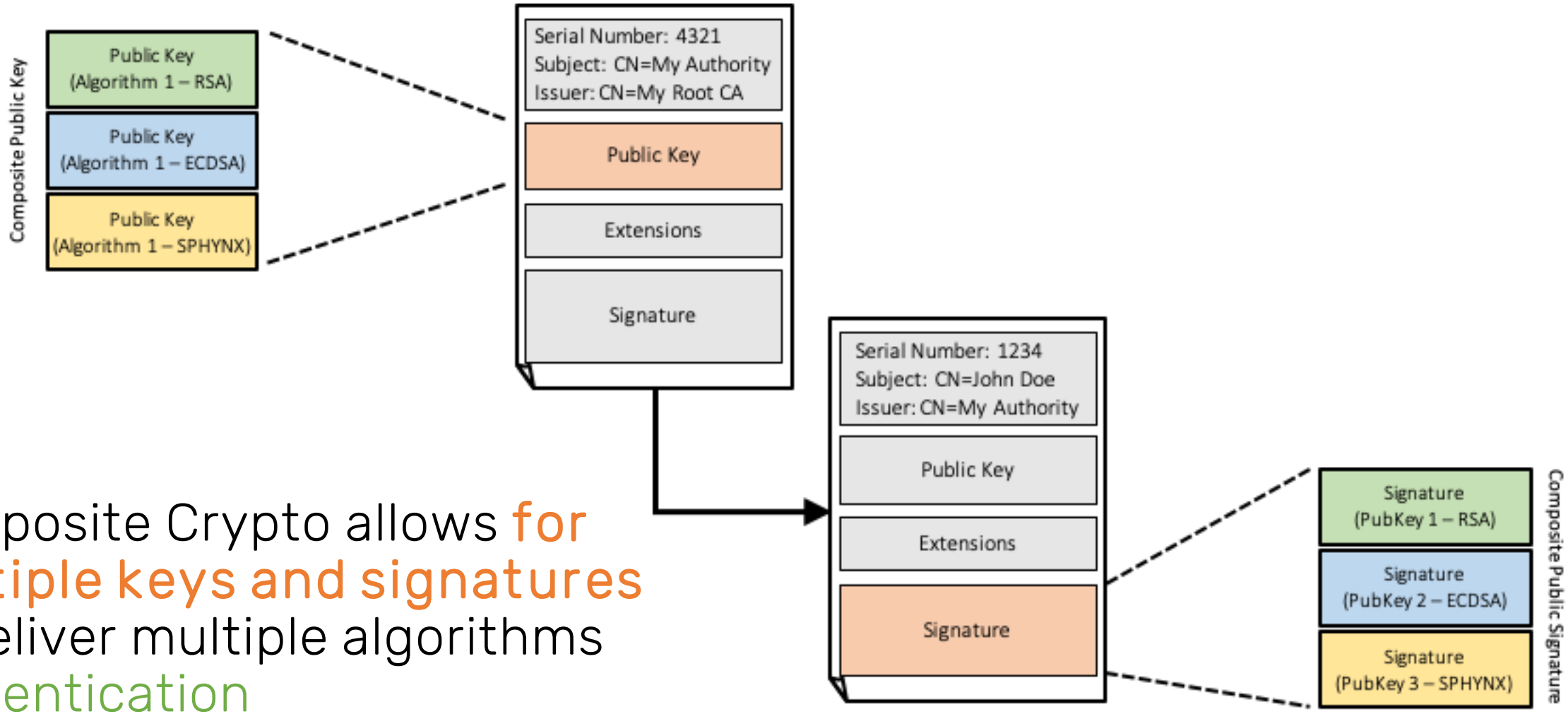
SCTE CABLE-TEC EXPO FAST FORWARD 2021
VIRTUAL EXPERIENCE
OCTOBER 11-14

Outline

- Multi-Key Certificates
  - Composite Crypto Limitations
  - Two Separate Data Structures
- Encryption Support
  - Composite Keys encryption
  - Combined Keys encryption
- Key Configuration Revocation
  - Key Configurations as OID sequences
  - Revocation Extensions
- Conclusions



Multi-Key Certificates

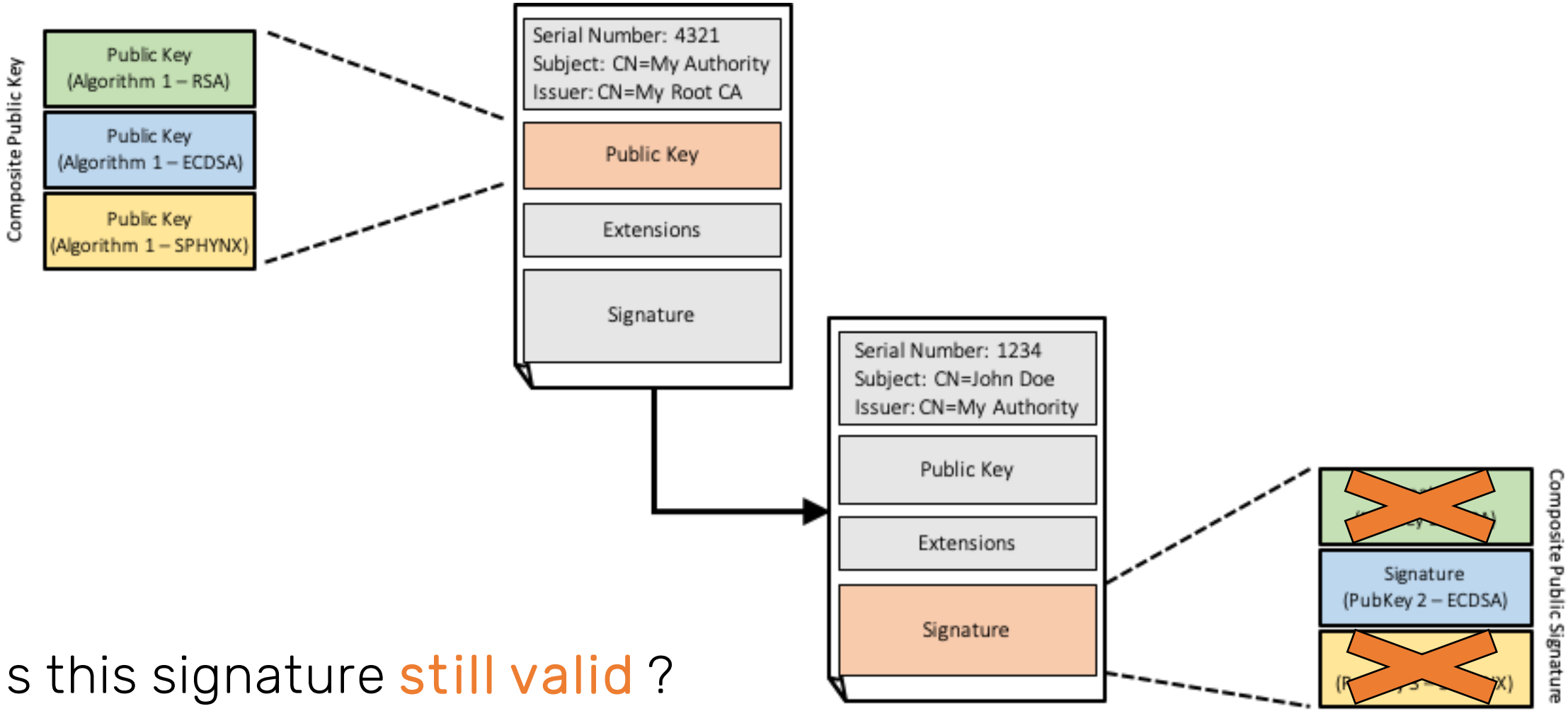


Composite Crypto allows for multiple keys and signatures to deliver multiple algorithms authentication

Uncertainty and Crypto APIs

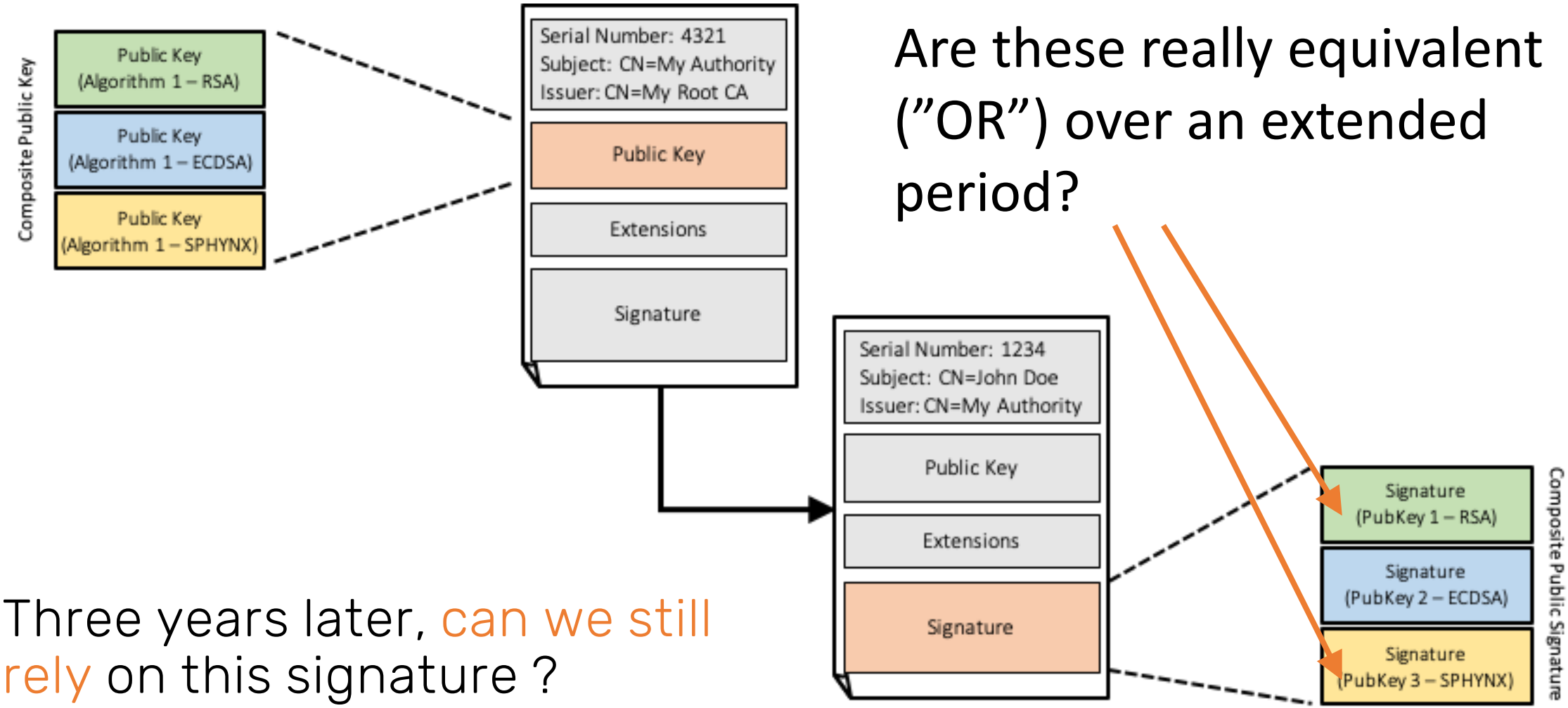
- When using multiple keys and error conditions are found, crypto libraries must have a clear indication of how to proceed
- Users and Crypto Libraries need indications about which algorithms are trusted and how to combine them together when signing and/or validating signatures

Multi-Key Certificates And Error Conditions



Is this signature still valid ?

Multi-Key Certificates And Time



Are these really equivalent (”OR”) over an extended period?

Three years later, can we still rely on this signature ?

We need a practical way to provide deterministic crypto library behavior

An Incomplete Paradigm ?

- In its original formulation we did not provide clear semantics associated with Composite Crypto
- Crypto libraries must change their APIs to support new error cases and crypto-policies validations
- How to distribute these policies across millions of devices?
- Because of the lack of deterministic behavior, even encryption has been currently excluded from current multi-key certificate scope

Composite & Combined Cryptography

- Instead of providing complex policies and associated data structures, we introduce a new type of multi-key public keys
- Same structure as Composite Crypto (different OID)
- The new structures for Keys and Signatures are referred to as Combined Crypto (i.e., Combined Keys and Combined Signatures)
- While Composite Crypto is used to implement the "OR" logic function among the components, the Combined Crypto is used to implement the "AND" logic function

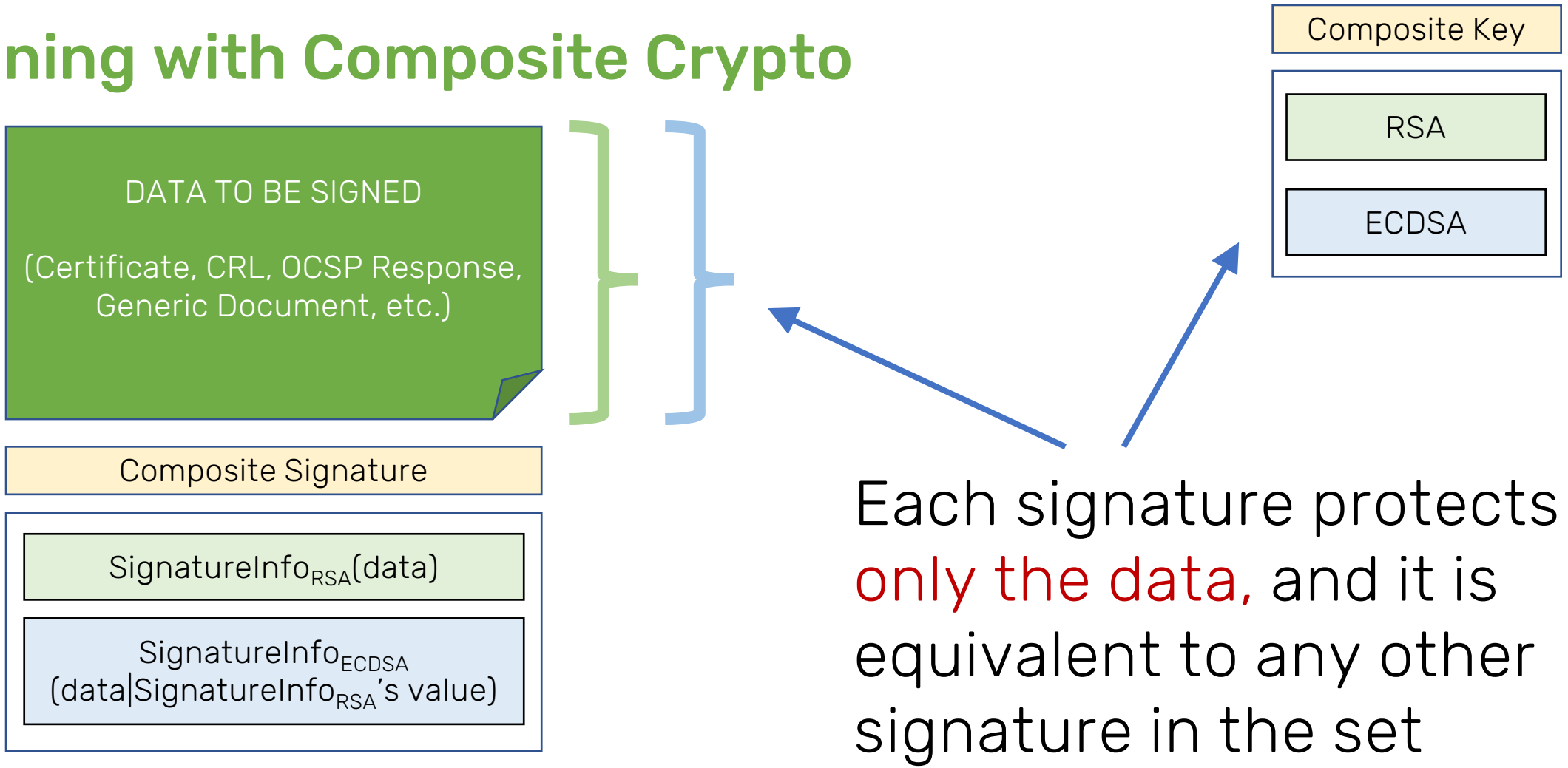
Composite Crypto

- When Signing, all Keys must be used to generate independently verifiable signatures
- When Validating a Composite Crypto signature, ANY of the individual signatures can be used to validate the signed data (OR)

Combined Crypto

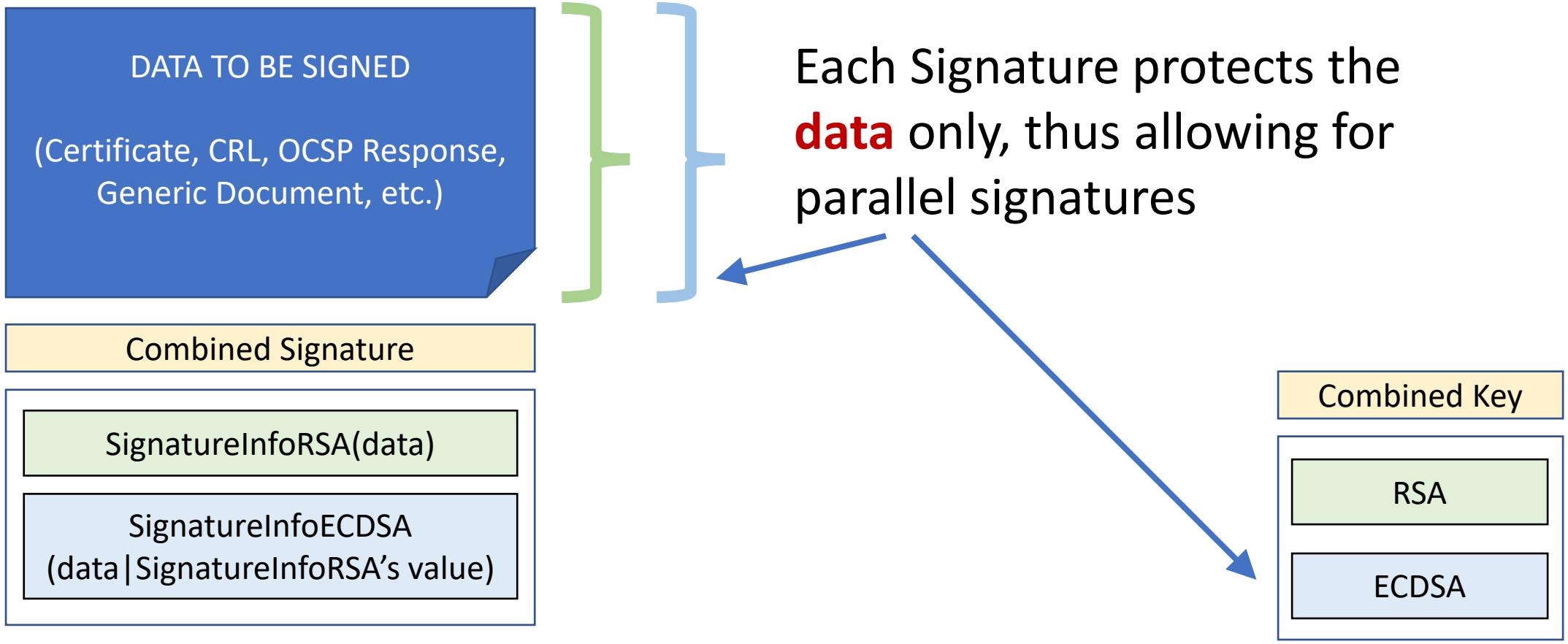
- When Signing, ALL Keys that support signing must be used to generate (NESTED signatures?).
- When Validating a Combined Crypto signature, ALL the individual signature must be correctly validated (AND)

Signing with Composite Crypto

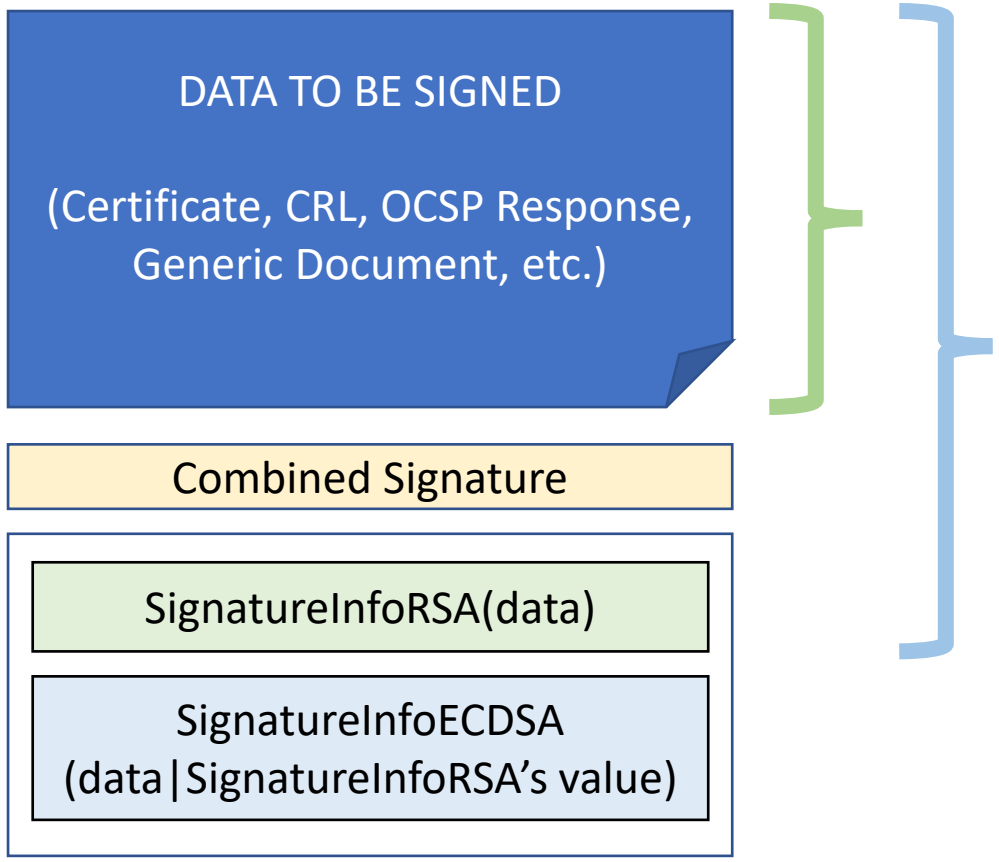


Each signature protects only the data, and it is equivalent to any other signature in the set

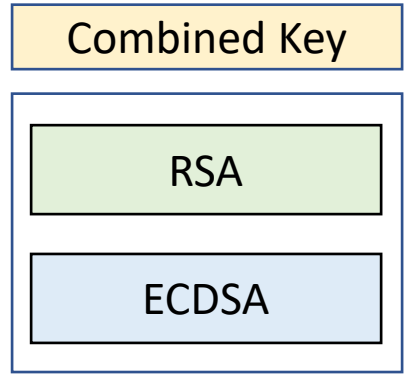
Not-Nested Signing with Combined Crypto



Nested Signing with Combined Crypto



Each Signature protects the data and the previous signatures in the "chain of signatures" values [*]



[*] prevents stripping when keys are not in a X.509 structure)

Enabling Encryption

- The use of Composite and Combined data structures also solves the ambiguity related to encryption and decryption
- We leverage the "OR" and "AND" logical operation to provide crypto libraries with deterministic behavior also for the Encryption processes
- A Composite Key is enabled for encryption if at least one of the components algorithms supports encryption.
- A Combined Key is enabled for encryption if all the components' algorithms support encryption.

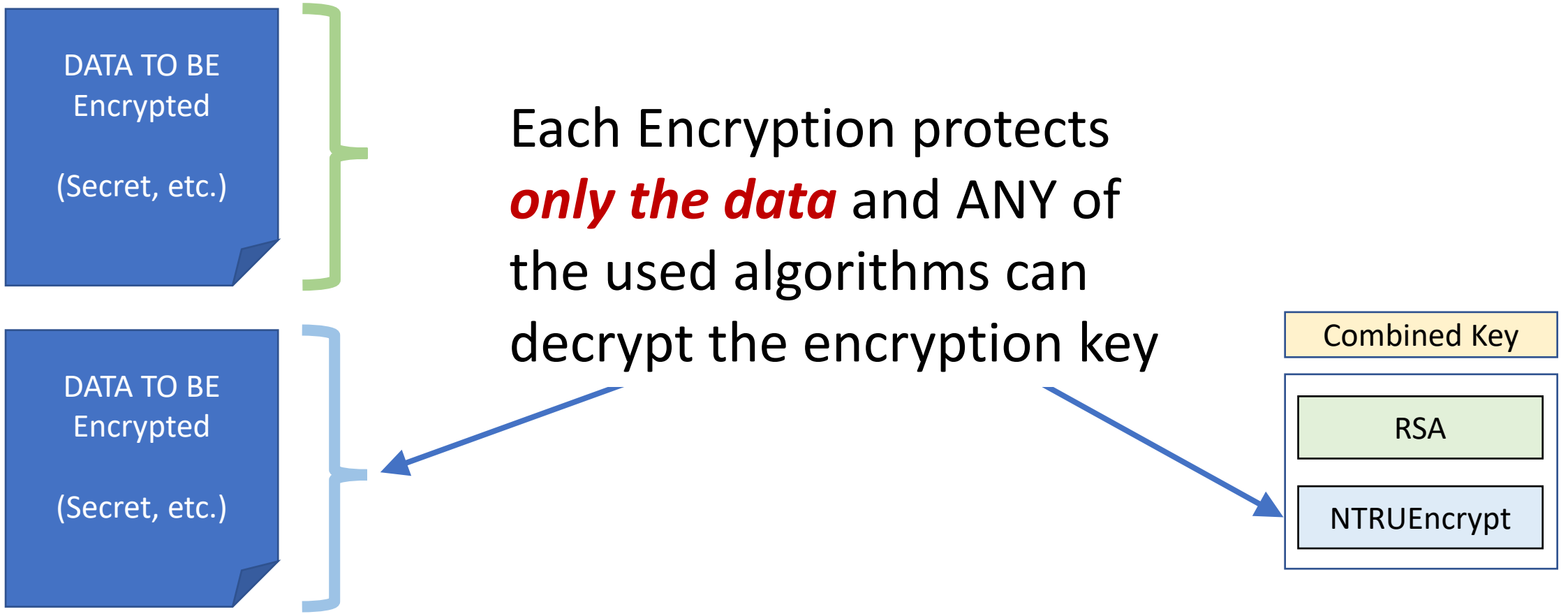
Composite Crypto

- When **Encrypting** for a Composite Key, the encryption is performed with all the public keys SEPARATELY
- When **Decrypting** with a Composite Key, the decryption can be performed with ANY of the private keys related to the single public key components (OR)

Combined Crypto

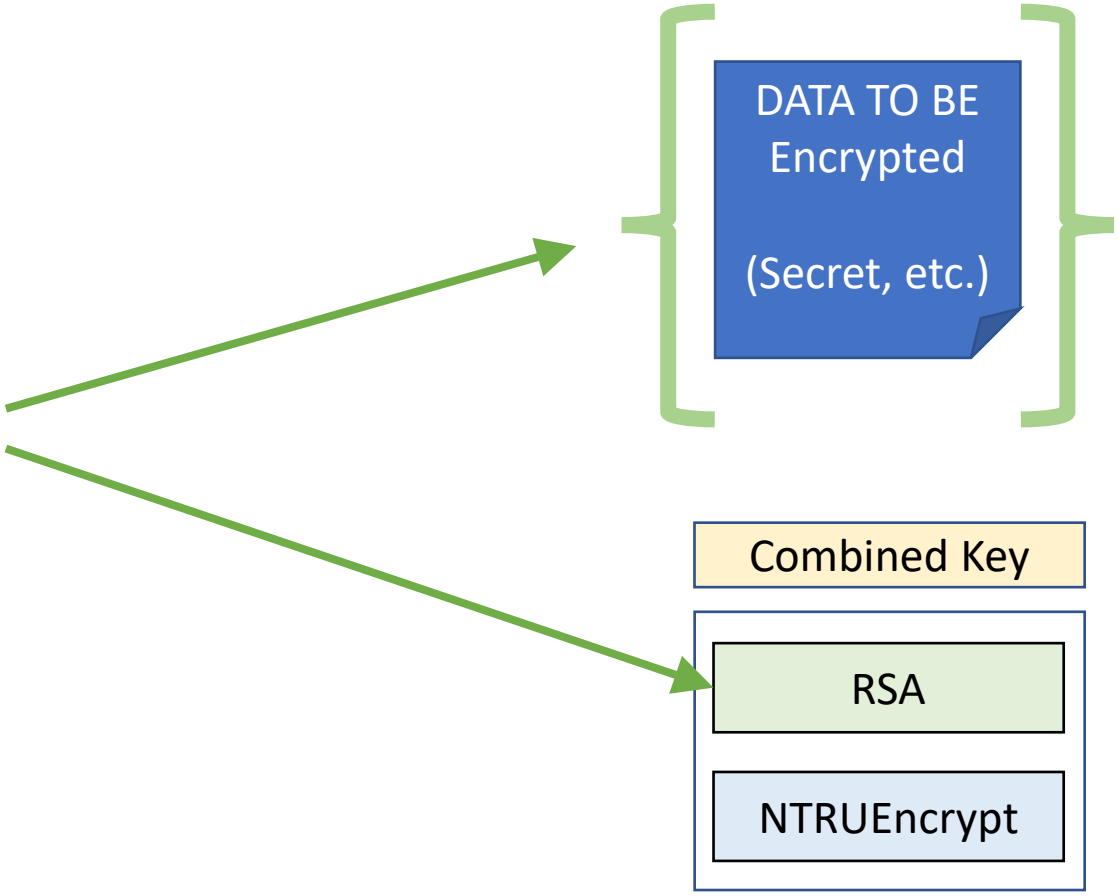
- When **Encrypting**, for a Combined Key, the encryption is performed by using all the public keys TOGETHER
- When Decrypting with a Combined Key, the decryption must be performed using ALL the private keys components of the combined key (AND)

Encrypting with Composite Crypto



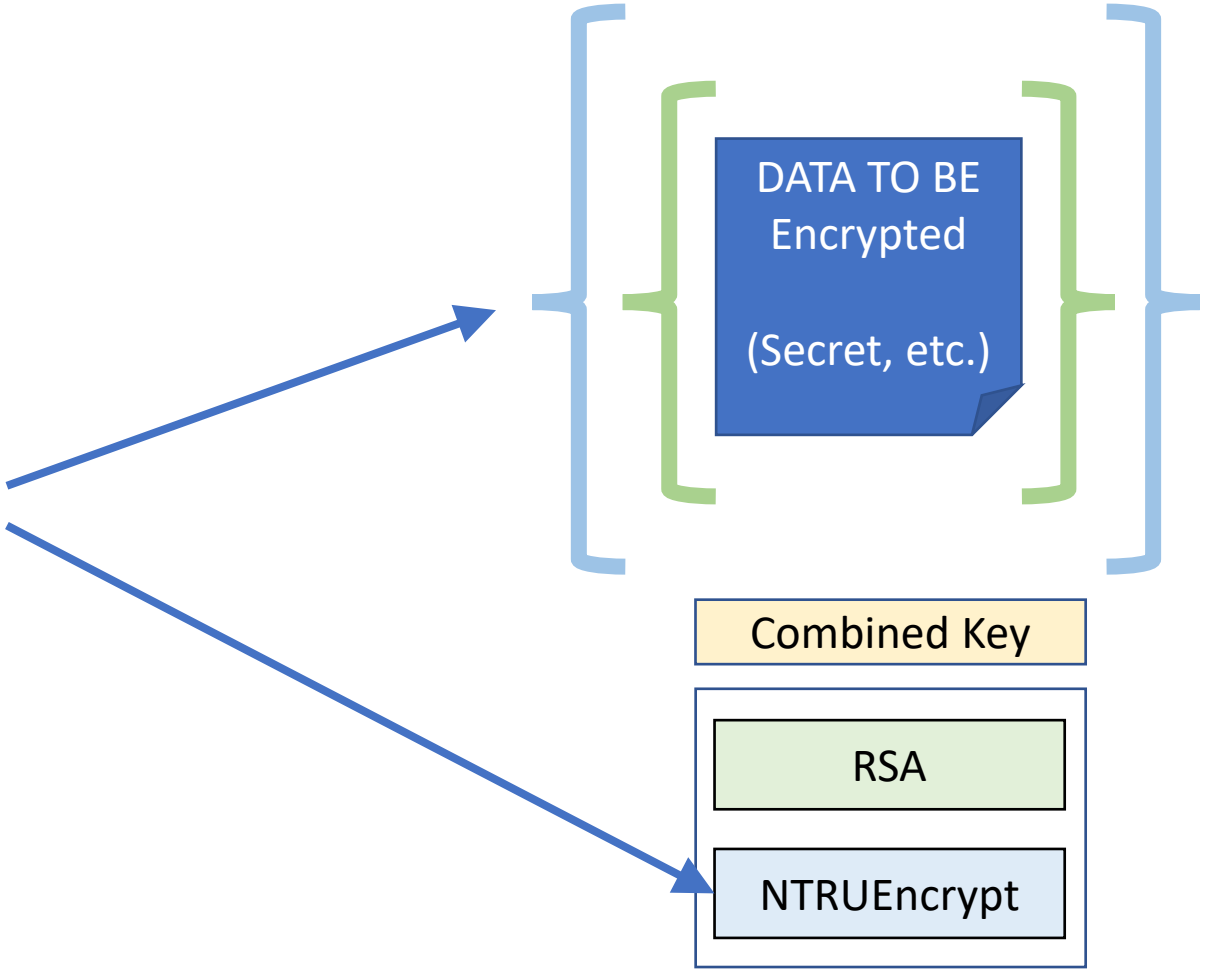
Nested Encrypting with Combined Crypto

The first Key in the Combined Key structure encrypts the data



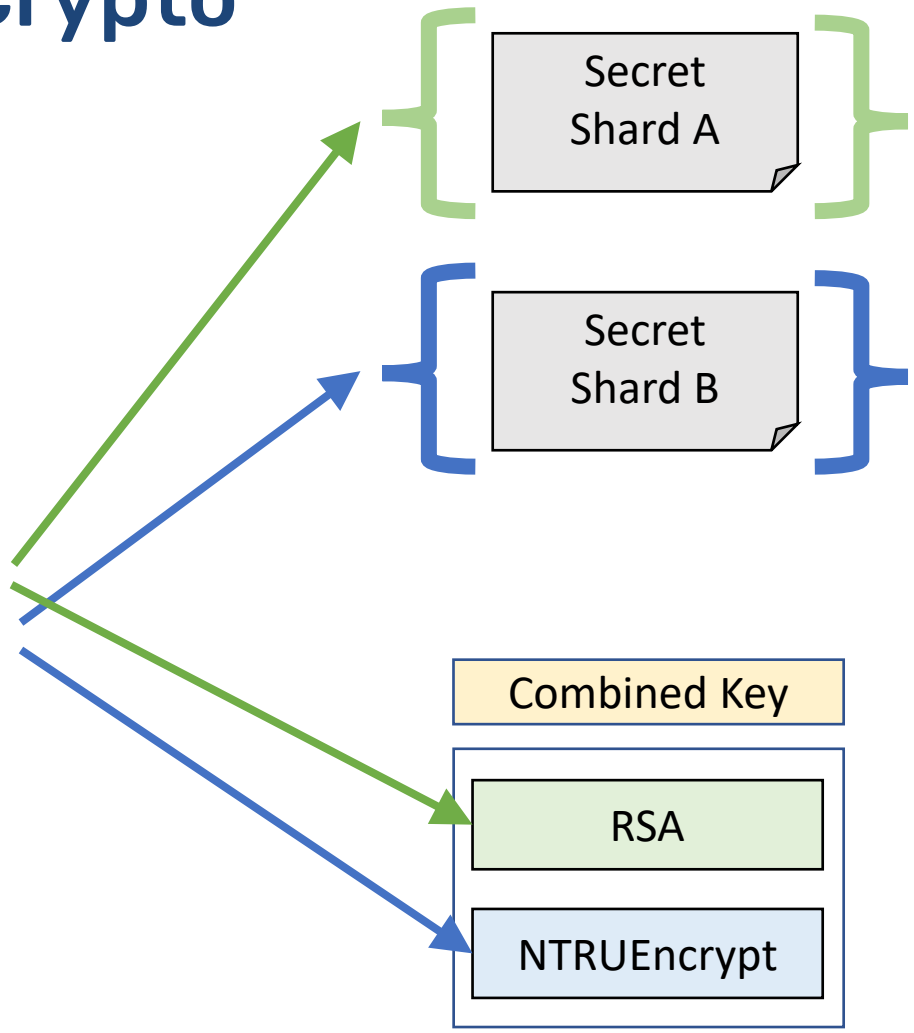
Nested Encrypting with Combined Crypto

Each subsequent Key in the Combined Key structure is used to encrypt the previous layer of protection in an "onion-like" encapsulation scheme



Nested Encrypting with Combined Crypto

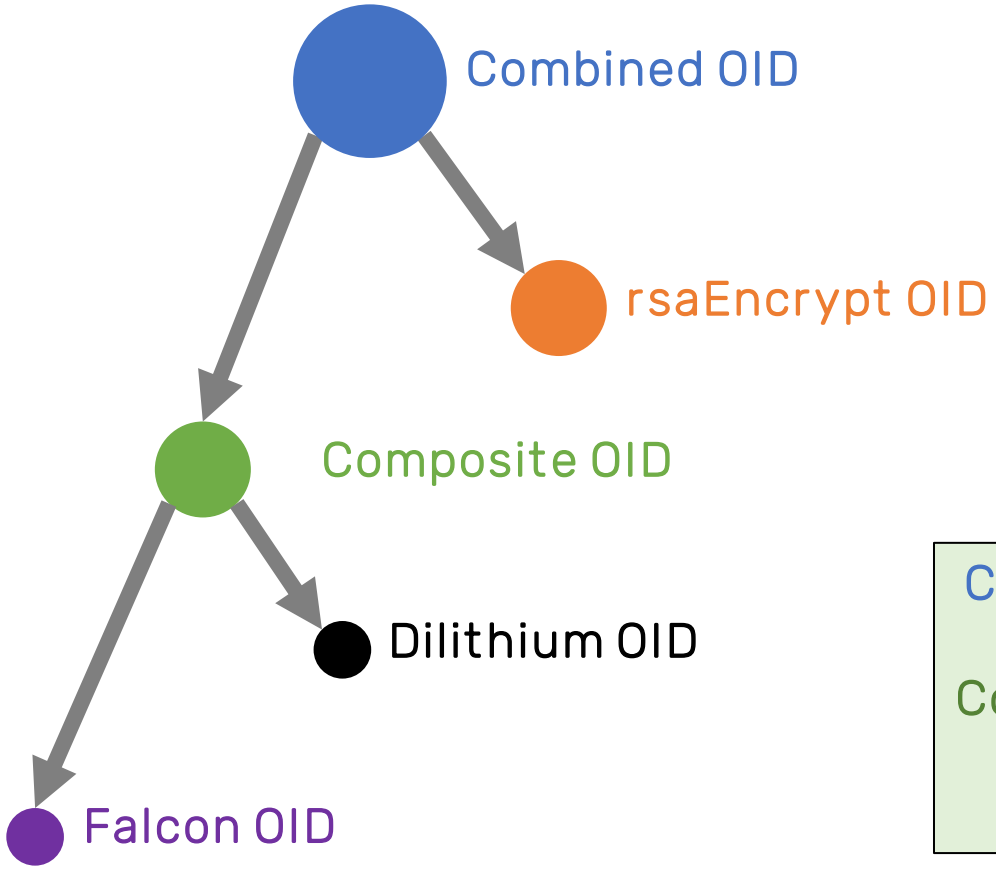
Each subsequent Key in the Combined Key structure is used to encrypt one of the key shards needed to reconstruct the secret/data



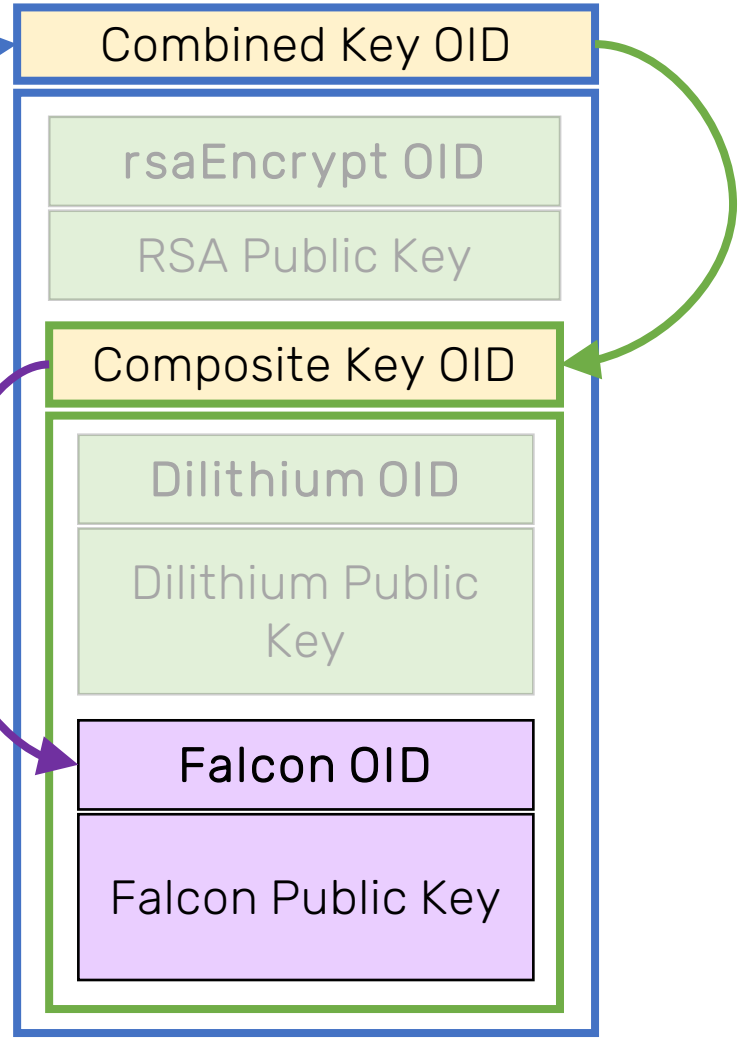
Surviving Algorithms' Failures

- When using multiple algorithms inside Keys, Signatures, and Encrypted Data, some of these algorithms might face total failures (like for the RSA problem and the quantum-computing threat)
- A mechanism is needed to provide the relying parties that are validating multi-key signatures (but this applies also to single-key certificates) with the indication of which algorithms (or which algorithm combinations) are considered not valid anymore (within the CA)
- The Revocation System can be leveraged to deliver such information safely and when needed – i.e., during certificate validation and from a trusted entity (the Issuing CA)

Key Structures as OID Trees

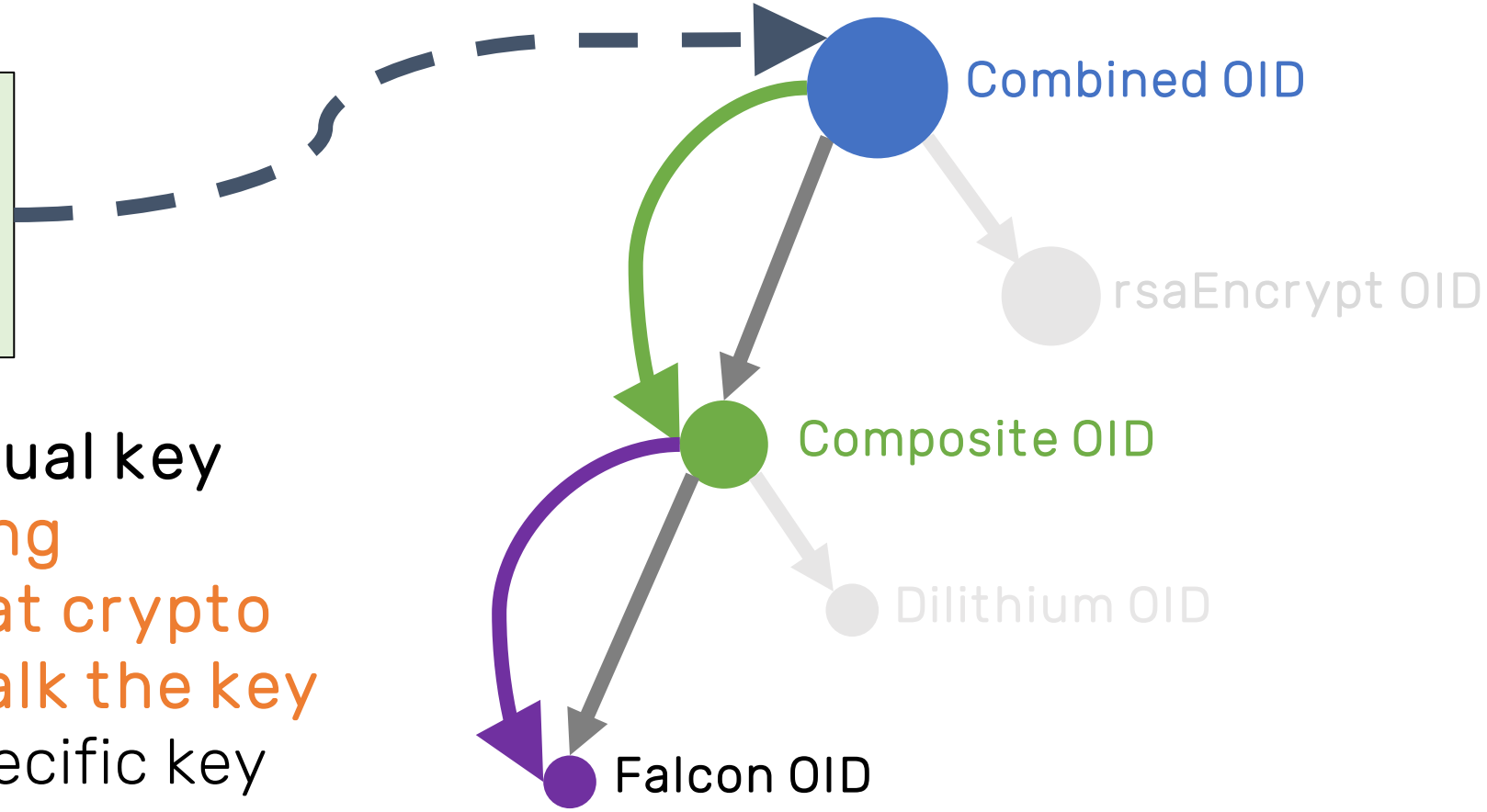


Combined Key OID
+
Composite Key OID
+
Falcon OID



Matching Keys via Tree Searches

Combined Key OID
+
Composite Key OID
+
Falcon OID



We can address **individual key configurations** by using sequences of OIDs that crypto libraries can use to walk the key structure up to the specific key component.

Conclusions

- Composite and Combined Crypto provide a complete definition of data structures and associated processing rules by implementing the “AND” and “OR” logic operations
- Different key configurations can be used in certificates to manage algorithm agility and algorithm failures over time.
- The structure of the public key provides clear authentication, validation, encryption, and decryption processing rules for crypto libraries
- CRLs and OCSP responses are used to carry sequences of OIDs (and validity periods) for individual key configuration revocation

SCTE® CABLE-TEC EXPO® FAST FORWARD 2021

ATLANTA, GA
OCTOBER 11-14

SCTE
a subsidiary of CableLabs®

Thank You!

Massimiliano Pala

PKI Architectures Team, Director
CableLabs

m.pala@cablelabs.com

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS