Multiple Public-Key Algorithm X.509 Certificates

draft-truskovsky-lamps-pq-hybrid-x509-00

A. Truskovsky
P. Lafrance
D. Van Geest

ISARA Corporation

S. Fluhrer
P. Kampanakis

Cisco Systems

M. Ounsworth
S. Mister
J. Gray

Entrust Datacard, Ltd

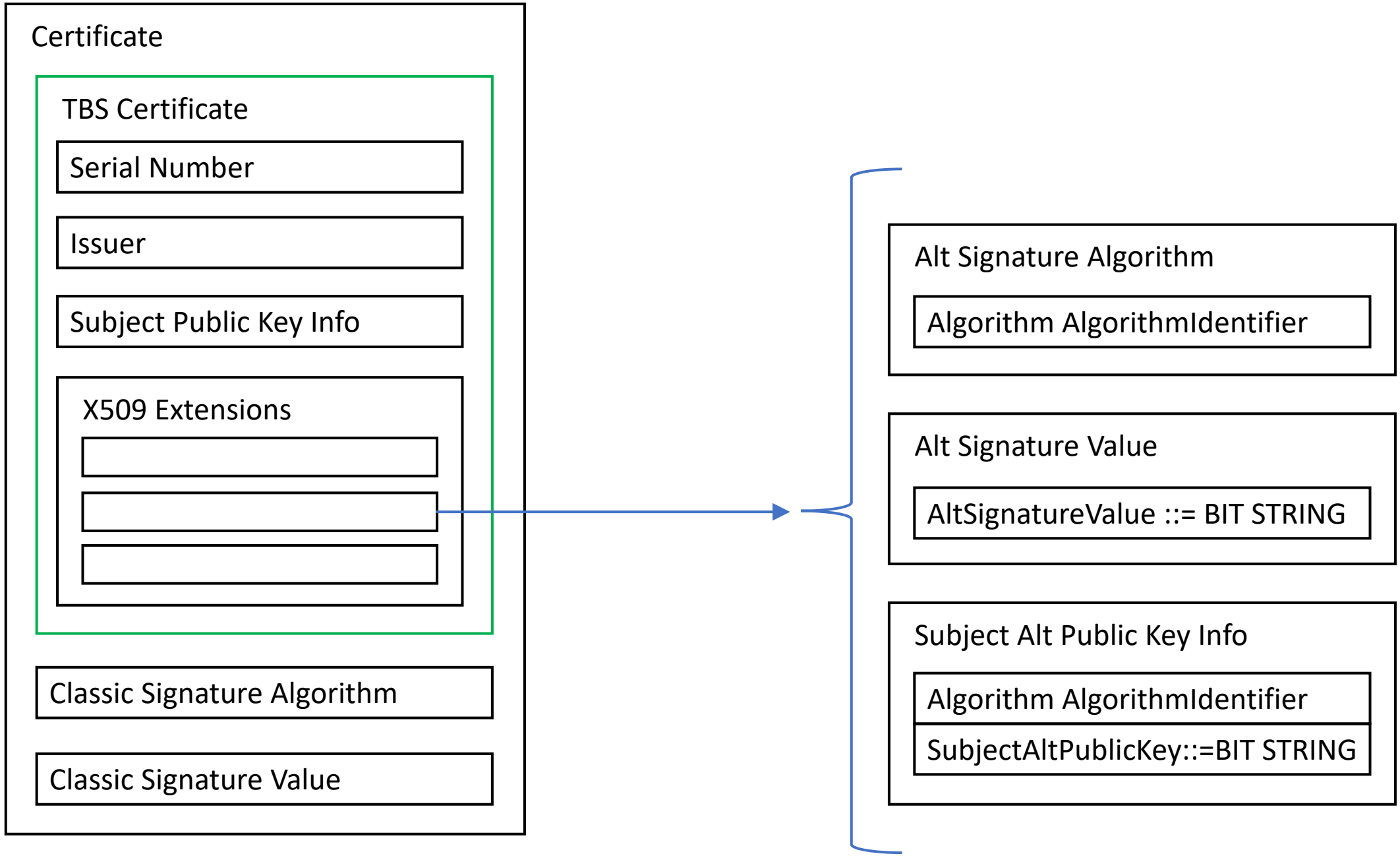
Motivation

- It will take several years to evaluate and select post-quantum algorithms
- Critical infrastructure will need to migrate to PQ algorithms in a short time-frame
- Non-upgraded legacy systems and clients will need to remain supported
- Algorithms used for key establishment are typically negotiated between peers and are easier to migrate
- Algorithms used for authentication are harder to migrate:
  - Public Key Infrastructure (PKI) often supports a variety of systems
  - X.509 certificate chain can only support a single algorithm in each certificate
- Make PKI more crypto agile to ensure a smoother migration
- Allow for a two-signature hybrid solution

Overview

- Supports multiple public key algorithms in each certificate of a certificate chain
- Upgraded systems with PQ algorithm support enabled can use PQ algorithms
- Non-upgraded legacy systems are able to continue using classic algorithms without any modification to them
- Alt signature algorithm, alt signature value and subject alt public key are placed in non-critical extensions
- Signatures are layered in such a way that all certificate attributes are covered by both signatures
- Classic signature is applied last, which makes the resulting certificates compatible with existing unmodified systems

```
X.509 Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4097 (0x1001)
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=CA, O=Test, CN=ECDSA-HSS-Hybrid-Test
        [ ... omitted for brevity ... ]
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            [ ... omitted for brevity ... ]
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            [ ... omitted for brevity ... ]
            Alt Signature Algorithm:
                 hss-with-SHA512
            Subject Alt Public Key Info:
                Leighton-Micali Hierarchical Signature System
                Public Key:
                    00:00:00: [ ... omitted for brevity ... ]
                Winternitz Value: 8 (0x00000004)
                Tree Height: 25 (0x00000009)
            Alt Signature Value:
                Signature:
                    30:82:0a:74: [ ... omitted for brevity ... ]
    Signature Algorithm: ecdsa-with-SHA256
         30:45:02:21:[ ... omitted for brevity ... ]
```


Certificate
TBS Certificate
Serial Number
Issuer
Subject Public Key Info
X509 Extensions
Classic Signature Algorithm
Classic Signature Value
Alt Signature Algorithm
Algorithm AlgorithmIdentifier
Alt Signature Value
AltSignatureValue ::= BIT STRING
Subject Alt Public Key Info
Algorithm AlgorithmIdentifier
SubjectAltPublicKey::=BIT STRING