On the Implementation of X509-Compliant Quantum-Safe Hybrid Certificates

Dimitrios Chatziamanetoglou
Obourg, 7034
Hainaut
BELGIUM
dimitrios.chatziamanetoglou@ncia.nato.int,
diehatz@cs.ihu.gr

Konstantinos Rantos
Ag. Loukas, 65404
Kavala
GREECE
krantos@cs.ihu.g r

ABSTRACT

With the rapid development of quantum computing, traditional cryptographic algorithms face an emerging threat, prompting the need for quantum-safe alternatives to ensure long-term security, especially in support of military operations in multiple domains. This paper explores the concept of hybrid X509 certificates that leverage a combination of traditional and post-quantum cryptographic algorithms for digital signatures. We present a proof-of-concept implementation utilizing a forked version of the OpenSSL library integrated with the Open Quantum Safe (OQS) library. Specifically, our implementation combines the ECDSA algorithm for traditional signatures with the post-quantum algorithm Crystals Dilithium, outlining the steps involved in generating, distributing, and verifying hybrid X509 certificates, highlighting the interoperability of the proposed solution with existing Public Key Infrastructure elements.

1.0 INTRODUCTION

The emergence of quantum computing has introduced a new dimension of security challenges. Traditional cryptographic algorithms, are soon to be vulnerable to attacks by entities which will possess quantum computing capacity. Therefore, the adoption of quantum-safe algorithms has become of paramount importance, especially in the areas of defence and security sectors.

The security and defence sectors, among other, are of critical strategic importance due to their significant role in safeguarding national and international interests. Compromises within those sectors can result to severe consequences for wide security and stability. To prevent unauthorized access, espionage, or sabotage, robust security measures are necessary to safeguard these assets and ensure their integrity.

Quantum-safe algorithms provide resistance against attacks from both classical and quantum computers, ensuring the long-term security of sensitive data and communications. By incorporating quantum-safe algorithms into the security infrastructure, security and defence sectors can mitigate the risks posed by quantum computing and maintain the confidentiality and integrity of critical information.

Hybrid X509 certificates containing both traditional and post-quantum algorithms are a promising solution to address the threat posed by quantum technology to traditional public key cryptography. In a hybrid certificate system, public and private keys are generated using both traditional and post-quantum algorithms which provides several advantages over traditional X509 certificates, underpinning a more secure and future-proof solution to address emerging threats posed by quantum technology, as well as it ensures backward compatibility with traditional public key cryptography systems, allowing a smooth transition period to post-quantum systems.

However, there are still some challenges that need to be addressed to fully realize the potential of hybrid X509 certificates. One challenge is the lack of standardization and interoperability between different hybrid

certificate systems, which can limit their wide application [1]. In addition, the increased overhead associated with post-quantum algorithms can impact the performance of public key infrastructure [2]

This paper, provides the details of a proof of concept (PoCt) implementation based on a fork of the openssl project, utilizing the open quantum safe (oqs) library, focusing on certificates for digital signatures, combining the traditional algorithm ECDSA and the post quantum algorithm Crystals-Dilithium. We outline the essential steps required for generating, distributing, and verifying hybrid X509 certificates of a trust chain consisting of a Root Certification Authority (CA) and an Intermediate CA, while supporting the creation of user's certificates, emphasizing the interoperability of the proposed solution.

Crystals Dilithium, has gained attention for its promising security against quantum attacks. Notably, the National Institute of Standards and Technology (NIST) has included Crystals Dilithium among its third-round result candidates for post-quantum cryptographic standards for digital signatures, along with FALCON and SPHINCS+ algorithms [3]. NIST's decision on selecting Crystals Dilithium demonstrates its robustness, further reinforcing its suitability for integration within hybrid X509 certificates.

2.0 QUANTUM-SAFE HYBRID CERTIFICATES

Digital signatures leverage security by providing authentication, integrity and non-repudiation of origin. It is used to authenticate the identity of the signer or originator of the data, validate the integrity of the data and the signer's signature, while provide proof of who actually was the signer of the data.

During the pre-quantum era, digital signature algorithms such as RSA, DSA, ECDSA etc were proven to be more than secure, but security concerns begun to arise when assumptions were made that attackers own quantum computers [4]. Post-quantum cryptography is the area of cryptography in which systems are studied under this security assumption, in which, all commonly used public-key algorithm-based systems are no longer secure.

In this transition period, we are going to face a dual folded challenge; there will be uncertainty on the algorithms security strength and also backwards compatibility cannot be ensured, as post-quantum algorithms will not be available by all clients. Furthermore, these algorithms come with strikingly different size and performance characteristics than their classical counterparts [5], [6]. During this transition, it is important to ensure a seamless cryptographic security, maintaining the current levels of security and functionalities, while exploring new ways of establishing and using hybrid certificates containing quantum-safe algorithms.

Instead of totally replacing current algorithms with arguably less-studied and less-supported post-quantum ones [7], the scientific community came up with 2 approaches, where the hybrid certificates will be used to bridge the gap between post-quantum and non-post-quantum enabled systems through versatility [8], while the ultimate goal is the usage of quantum safe cryptography, pending though the final results of the evaluation of such algorithms.

The first one, which will be the subject of the present paper, consists of combining a traditional and a post-quantum algorithm into the same X509 fields by concatenating the shared secrets, where the overall system's security is lower bounded by the stronger of the two cryptosystems [9].

The second one, which is outside the scope of this paper, is the use of hybrid X509 certificates extending the schema of the present certificate structure with additional extensions, containing post-quantum algorithms, in addition to the traditional ones [10]. By marking the additional certificate extension as non-critical, existing PKI infrastructure (not aware of the hybrid structure) should ignore the unrecognized extension and continue validating the certificate based on the traditional algorithm and using it in applications without change.

3.0 APPLICATION IN THE DEFENCE SECTOR

Digital signatures are pivotal cryptographic tools essential for ensuring the security, accountability, and reliability of military operations. These signatures serve as a trusted mechanism for verifying the authenticity of message senders, protecting data integrity against tampering, and establishing non-repudiation to hold individuals accountable for their actions.

One of the primary functions of digital signatures in military operations is authentication. By using public-key cryptography, digital signatures verify the legitimacy of message senders. Furthermore, digital signatures safeguard the integrity of data during its transmission or storage. This is especially crucial in military contexts where the tampering of mission-critical information can have dire consequences. Digital signatures also ensure non-repudiation, a cornerstone of accountability in military operations, making it impossible for message senders to later deny the authenticity of their digital signature. This level of assurance is vital when it comes to actions and decisions made during military operations.

Quantum-safe digital signature algorithms, introduces a paradigm shift in the realm of military operations by enhancing security and resilience in an era characterized by the growing capabilities of quantum computers. These cryptographic advancements provide overarching benefits to military communications by ensuring the confidentiality, integrity, and authenticity of sensitive information by providing robust protection against quantum attacks.

While the robustness of the new quantum-safe algorithms is yet to be proved, the defence sector can be prepared and lead the applicability of this new technology due to the sensitivity of data of the military context. Especially now, when the quantum technology is emerging and the risk of "harvest now and decrypt later" is more than evident.

The application examples in the defence sector context can vary, starting from network security in general, where military networks support all kind of information exchange and command and control in modern multi domain operations. Unmanned Aerial Vehicles (UAVs) is another example, where related missions are indispensable for modern military reconnaissance and surveillance activities. Furthermore, the examples can be extended to submarine operations, operating in challenging underwater environments where secure communication is vital, where quantum-safe digital signatures can enhance the authentication and integrity of messages exchanged with naval command centres, ensuring that submarines can rely on the legitimacy of commands, even when faced with unreliable communication channels.

In that context, and highlighting the fact that Public Key Infrastructure is a vital component of modern military communications, we demonstrate the creation of a hybrid PKI, using both traditional and quantum-safe algorithms, underpinning the security of military operations in all domains.

4.0 PROOF-OF-CONCEPT (POCT)

As mentioned before, we selected to build our proof of concept utilizing a forked version of the OpenSSL library integrated with the Open Quantum Safe (OQS) library [11], including algorithms such as lattice-based, code-based, multivariate polynomial-based, and other post-quantum cryptographic schemes. Furthermore, the produced certificates are fully compatible with the latest recommendations of ITU-T [12].

It needs to be clear, that this approach does not affect any data applicable to the conventional information of the digital certificate. On the contrary, it proposes that the additional information for the post-quantum algorithms use the X509 current structure fields as a vehicle to store the post-quantum information using the concatenation method, allowing the existence of both traditional and quantum-safe algorithms within a single certificate, enabling the coexistence of different cryptographic schemes.

4.1 Overview of the Certificate Chain of Trust

A certificate chain of trust, also known as a trust chain or certification path, is a hierarchical sequence of digital certificates used to establish the authenticity and integrity of a digital entity. The certificate chain of trust, ensures that entities relying on digital certificates can confidently trust the identity and integrity of the entities they are communicating with, forming the foundation of secure online transactions, secure communication channels, and digital trust ecosystems.

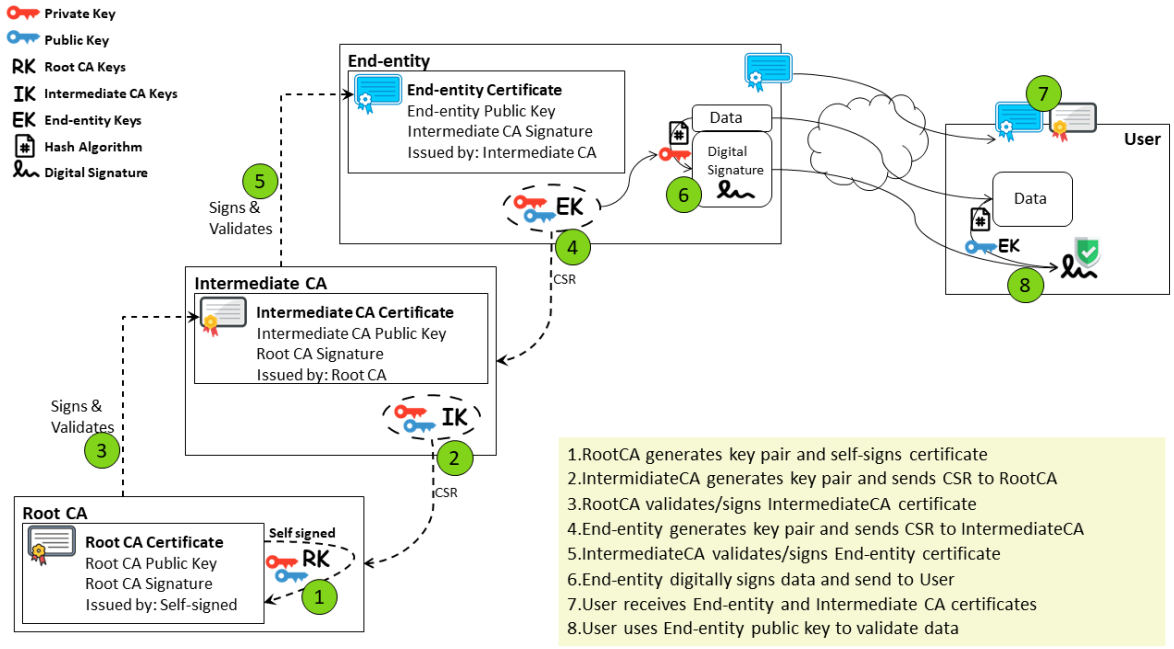

Figure 1: PKI trust chain.

4.2 Proof-of-Concept Implementation

The PoCt was created on a virtualized environment hosted on a VMware ESXi 7.0 U2 hypervisor, based on Ubuntu Linux (64-bit) as OS with 8 CPUs and 12 GB of memory. Our implementation combines the ECDSA algorithm for traditional signatures with the post-quantum algorithm Crystals Dilithium 5.

4.2.1 Create RootCA (*offline process)

Create a RootCA Private Key and a self signed RootCA Certificate

apps/openssl req -x509 -newkey p521_dilithium5 -keyout sto/RootCAkey_ecdsa_dil5.pem -out sto/RootCAcert_ecdsa_dil5.pem -config apps/openssl.cnf

4.2.2 Create IntermediateCA

Create Extension Parameters

Create extension file for including x509 v3 extension parameters when singed from RootCA, otherwise the full trust chain of the user verification will not be successful. Create sto/ca_intermediate.ext file with the following content:

```
[ v3_intermediate_ca ]
# Extensions for a typical intermediate CA
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
```

Create an IntermediateCA private key and an IntermediateCA Certificate Signing Request (CSR)

```
apps/openssl req -newkey p521_dilithium5 -keyout sto/IntermediateCAkey_ecdsa_dil5.pem -out sto/IntermediateCAcsr_ecdsa_dil5.csr -config apps/openssl.cnf
```

Create IntermediateCA certificate by signing it with RootCA certificate

```
apps/openssl x509 -req -in sto/IntermediateCAcsr_ecdsa_dil5.csr -CA sto/RootCAcert_ecdsa_dil5.pem -CAkey sto/RootCAkey_ecdsa_dil5.pem -out sto/IntermediateCAcert_ecdsa_dil5.pem -extfile sto/ca_intermediate.ext -extensions v3_intermediate_ca
```

Verify IntermediateCA certificate against RootCA certificate

```
apps/openssl verify -CAfile sto/RootCAcert_ecdsa_dil5.pem sto/IntermediateCAcert_ecdsa_dil5.pem
```

4.2.3 Create User Certificate

Create user key pairs and CSR

```
apps/openssl req -newkey p521_dilithium5 -keyout sto/User1key_ecdsa_dil5.pem -out sto/User1csr_ecdsa_dil5.csr -config apps/openssl.cnf
```

Create User certificate by signing it with IntermediateCA certificate

```
apps/openssl x509 -req -in sto/User1csr_ecdsa_dil5.csr -CA sto/IntermediateCAcert_ecdsa_dil5.pem -CAkey sto/IntermediateCAkey_ecdsa_dil5.pem -out sto/User1cert_ecdsa_dil5.pem
```

Verify user certificate against IntermediateCA certificate

```
apps/openssl verify -CAfile sto/RootCAcert_ecdsa_dil5.pem -untrusted sto/IntermediateCAcert_ecdsa_dil5.pem sto/User1cert_ecdsa_dil5.pem
```

4.3 Hybrid Certificate Structure

As already mentioned, the structure of the produced hybrid certificates is not altered and remains compatible to the latest ITU-T recommendation. The additional information of the quantum-safe algorithms, such as the public key and the digital signature are concatenated with the respective elements of the traditional algorithms.

The basic contents of an X509, following the ASN.1 structure is as follows [13] (some elements are omitted for brevity reasons):

```
Certificate ::= SEQUENCE {
        tbsCertificate          TBSCertificate,
        signatureAlgorithm      AlgorithmIdentifier,
        signatureValue          BIT STRING }

TBSCertificate ::= SEQUENCE {
        version                 Version,
        serialNumber            CertificateSerialNumber,
        signature               AlgorithmIdentifier,
        issuer                  Name,
        validity                Validity,
        subjectPublicKeyInfo    SubjectPublicKeyInfo,}

SubjectPublicKeyInfo ::= SEQUENCE {
        algorithm               AlgorithmIdentifier,
        subjectPublicKey        BIT STRING }

AlgorithmIdentifier ::= SEQUENCE {
        algorithm               OBJECT IDENTIFIER,
        parameters              ANY DEFINED BY algorithm OPTIONAL
}

Version ::= INTEGER { v1(0), v2(1), v3(2) }
```

In our case, the public key value of the hybrid certificate is the concatenated value of the ECDSA p521 algorithm with the respected value of Dilithium5, *subjectPublicKey=Pub(ECDSA_p521) || Pub(Dilithium5)*. In addition, the signature value of the hybrid certificate is the concatenated value of the utilised aforementioned algorithms, thus *signatureValue=Sig(ECDSA_p521) || Sig(Dilithium5)*. Once the ASN.1 content is DER (Distinguished Encoding Rules) encoded into binary format, TLV (Tag, Length, Value) information is included in order to distinguish where the traditional algorithm elements end and the post-quantum algorithm elements begin.

Accordingly, one of the quantum-safe hybrid certificates produced in our PoCt facility is shown below. The RootCA certificate was chosen for demonstrating reasons, however all the rest of the certificates follow similar structure and content.

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      4a:24:de:52:e3:9f:cf:f9:e7:12:fc:6c:77:1d:c4:f0:ac:86:fb:64
    Signature Algorithm: p521_dilithium5
    Issuer: C = AU, ST = Some-State, O = RootCA
    Validity
      Not Before: Jun  8 18:46:55 2023 GMT
      Not After : Jun  8 18:46:55 2024 GMT
    Subject: C = GR, ST = Thessaloniki, O = RootCA
    Subject Public Key Info:
     Public Key Algorithm: p521_dilithium5
        Public-Key: (521 bit)
        pub:
        04:00:65:8f:87:b9:fc:15:a5:25:f4:f5:e5:66:56:7b:d3:14:43:27:a6:9f:73:ae:6c:00:53:5c:c0:2f:   2 Bytes ASN1 prefix
        04:03:37:af:0d:e0:a7:2e:64:fa:0c:81:4e:33:ff:b0:37:6f:07:97:07:5e:7c:55:2c:80:47:19:e6:69:   131 Bytes ECDSA Public Key
                                    … omitted for brevity …
        0f:03:19:10:73:4d:79:4b:fb:1a:84:23:7a
        ASN1 OID: secp521r1
        NIST CURVE: P-521
        dilithium5 Public-Key:
        pub:
        4f:a8:b9:c7:c9:fa:df:e4:26:0e:77:c6:44:37:94:5b:8c:6c:04:bd:7d:a0:50:40:27:39:ab:07:8c:95:
        fb:37:65:fc:8a:be:d3:52:00:0a:69:62:cc:35:31:cf:3b:55:f4:65:6a:d8:eb:b0:73:49:10:7d:ed:c3:
        9b:c7:5b:26:2b:bd:76:4f:93:14:0f:a0:16:2a:30:39:8b:99:fb:b9:7d:a3:46:cb:b8:ac:06:78:b6:d4:   2592 Bytes Dilithium5 Public Key
                                    … omitted for brevity …
        d7:51:19:6a:bc:9c:ee:37:27:9c:62:77:ca:26:ec:13:38:2b:2b:e6:3c:c2:06:47:d7:01:f6:ed:95:0b:
        f1:00:fb:c6:d0:8f:1a:d3:ef:ea:88:9e
    Signature Algorithm: p521_dilithium5
     00:00:00:8a:30:81:87:02:41:51:6b:60:d6:05:0c:9b:68:f1:5d:eb:d0:28:12:3b:70:65:af:76:c6:69:   10 Bytes ASN1 prefix
     f5:fd:c7:d3:d9:60:d9:9f:5c:89:d5:a7:0f:1c:dd:b7:f8:b6:5d:7b:cf:67:1a:bb: cc:07:a0:3e:45:57:aa:   132 Bytes ECDSA Signature
                                    … omitted for brevity …
     21:42:3a:38:62:55:bd:dd:d2:9b:65:93:66:3e:0d:f2:b6:04:94:df:d2:55:18:83:c8:e9:9d:94:6d:0a:
     9d:38:c6:ee:4e:2f:fe:44:27:e6:cd:41:db:42:3c:62:5f:ce:dd:1f:94:94:62:d2:2d:36:c3:49:dd:de:8a:
     d4:30:1b:50:31:c2:a1:8f:4f:b4:6d:e8:0d:5c:0c:dd:31:a5:a4:95:ba:81:ef:35:16:b4:6f:f9:d5:4c:86:   4595 Bytes Dilithium5 Signature
                                    … omitted for brevity …
     f7:00:35:5d:89:d1:d2:06:0e:13:ae:c6:0d:28:2d:74:96:b3:24:7f:95:b6:d8:00:0e:62:6b:79:8b:96:
     e7:e8:2d:36:60:f0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0c:1b:21:26:2c:31:3a:3e
```

Concatenated Public Keys TLV Separated

Concatenated Signatures TLV Separated

5.0 CONCLUSION

The security and defence sectors are facing a pressing concern regarding the current cryptographic algorithms in the face of quantum computers. The breakthrough of these algorithms necessitates the availability of quantum computers with increased performance capacity, while the exact timeline for their widespread availability remains uncertain.

Today, much of the information we communicate is encrypted using public-key cryptography algorithms that are susceptible to attacks by quantum computers. This emerging vulnerability raises concerns that persistent threats or even state-sponsored hackers may be already intercepting and storing encrypted messages with the anticipation of decrypting them in the future when quantum computing resources become available. To address this looming threat, it is crucial to expedite the migration to post-quantum cryptographic algorithms.

In the present paper, we have presented a hybrid Proof of Concept Public Key Infrastructure combining traditional and post-quantum algorithms, demonstrating that a remarkable foundation work has already been progressed, which still is under development.

The migration to post-quantum cryptographic algorithms requires meticulous planning and global coordination and collaboration. This process entails various aspects, including education, training, and raising awareness about the need for quantum-resistant cryptography. Extensive coordination among stakeholders involved in the design and development of hardware, software, and IT infrastructure components is vital. By preparing early, the transition to post-quantum cryptographic algorithms can be executed in a cost-effective and efficient manner, minimizing disruptions and ensuring the continued security of the security and defence sectors' critical information.

6.0 REFERENCES

[1] I. Kong, "Transitioning towards quantum-safe government: Examining stages of growth models for quantum-safe public key infrastructure systems," in Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, 2022, pp. 499–503.

[2] M. Kumar, "Post-quantum cryptography algorithm's standardization and performance analysis," Array, vol. 15, p. 100242, 2022.

[3] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta et al., "Status report on the third round of the nist post-quantum cryptography standardization process," US Department of Commerce, NIST, 2022.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997. [Online]. Available: https://doi.org/10.1137/S0097539795293172

[5] P. Kampanakis, P. Panburana, E. Daw, and D. V. Geest. The viability of post-quantum X.509 certificates. Cryptology ePrint Archive, Report 2018/063, 2018. https://eprint.iacr.org/2018/063.

[6] P. Kampanakis and T. Lepoint, "Do we need to change some things? open questions posed by the upcoming post-quantum migration to existing standards and deployments," Cryptology ePrint Archive, 2023.

[7] J. Park, N. N. Anandakumar, D. Saha, D. Mehta, N. Pundir, F. Rahman, F. Farahmandi, and M. M. Tehranipoor, "Pqc-sep: Power side-channel evaluation platform for post-quantum cryptography algorithms," Cryptol. ePrint Arch., Tech. Rep, vol. 527, p. 2022, 2022.

[8] E. Crockett, C. Paquin, and D. Stebila, “Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH”, Cryptology ePrint Archive, 2019

[9] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, “Transitioning organizations to post-quantum cryptography,” Nature, vol. 605, no. 7909, pp. 237–243, 2022.

[10] N. Bindel, U. Herath, M. McKague, and D. Stebila, “Transitioning to a quantum-resistant public key infrastructure” in International Workshop on Post-Quantum Cryptography. Springer, 2017, pp. 384–405.

[11] D. Stebila and M. Mosca, “Post-quantum key exchange for the internet and the open quantum safe project.” In Roberto Avanzi, Howard Heys, editors, Selected Areas in Cryptography (SAC) 2016, LNCS, vol. 10532, pp. 1–24. Springer, October 2017, https://openquantumsafe.org.

[12] ITU-T, "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks", Recommendation ITU-T X.509, October 2019

[13] R. Housley, W. Ford, W.Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280, May 2008. https://tools.ietf.org/html/rfc5280