Using Attribute Certificates to Support Cryptographic Algorithm Flexibility

Steffen Fries, Rainer Falk
Siemens AG
Technology
Munich, Germany
e-mail: {steffen.fries|rainer.falk}@siemens.com

***Abstract*—Asymmetric cryptography is broadly used to protect confidentiality, integrity, and authenticity of data transfer. Typical applications are authentication and key agreement in secure communication protocols, and digital signatures for authentication and integrity protection of documents and messages. Digital certificates confirm the public key of a user. They are used for user authentication performed during the handshake by common cryptographic security protocols like Transport Layer Security, Datagram Transport Layer Security, or by authentication and key agreement protocols like the Internet Key Exchange or Group Domain of Interpretation. The cryptographic algorithm for public-key-based user authentication is fixed by the user's certificate. More flexibility to support multiple cryptographic algorithms for user authentication is needed, e.g., by the introduction of new, quantum-safe cryptographic algorithms. Attribute certificates can be used to support flexibly multiple cryptographic algorithms for user authentication, supporting a stepwise transition towards newer cryptographic algorithms.**

Keywords–communication security; cryptographic agility; post-quantum cryptography; attribute certificates; industrial automation and control system; Internet of Things; automation control systems.

I. INTRODUCTION

Asymmetric cryptography and digital signatures are a cornerstone in many security architectures. Main applications of digital signatures are user (entity) authentication and integrity protection of data at rest and in transit. The user utilizes his private key for authentication. A peer verifies the authentication using the corresponding public key. Digital certificates, e.g., according to the X.509 standard, confirm the user identity associated with the user's public key [1].

Besides entity authentication, digital signatures provide integrity protection of the signed content, which may be a document or, in case of the initial phase of security protocols, protect the negotiation of security parameters for a communication session as used in common security protocols like Transport Layer Security (TLS) [2] and Datagram Transport Layer Security (DTLS) [3], or in "pure" authentication and key agreement protocols like the Internet Key Exchange (IKEv2) [4] or the Group Domain of Interpretation GDOI) [5] protocol.

Due to advances in quantum computing, currently used asymmetric cryptographic algorithms like RSA (Rivest, Shamir, Adleman) or ECDSA (Elliptic Curve Digital Signature Algorithm) are endangered, as there underlying mathematical problems, like factorization and discrete logarithm problems (see also [6]) can be solved efficiently using a cryptographically relevant quantum computer leveraging Shor's algorithm (see also [7]). Symmetric cryptographic algorithms can also be attacked using Grover's algorithm (see also [7]), but for them it is currently seen sufficient to double the key length without a change of the algorithms (see also [8]).

While the standardization and the journey to introduce new, post-quantum asymmetric algorithms that withstand such attacks is still ongoing, the discussion of transition approaches for currently used cryptographic algorithms to new algorithms has already started (see [9]). In this context, different strategies are being discussed, like the combined or hybrid use of classical and post-quantum algorithms. This also relates to the utilized credentials, which may come in different formats like hybrid certificates supporting alternative cryptographic algorithms in the same certificate (see [1]). However, only a single second public key of a single second cryptographic algorithm can be included. As multiple quantum-safe cryptographic algorithms are currently standardized, a more flexible approach to support multiple public keys for authentication of a single user is needed.

Note that the case of post-quantum cryptographic algorithms is taken here as example. Crypto agility as the ability to adopt to alternative cryptographic algorithms, is a general design objective for protocols and architectures to ensure that new algorithms with similar boundary conditions can be deployed easily.

Transition is specifically important for industrial use cases, as the component lifetime here is much longer compared to consumer electronics. Therefore, it is important to elaborate ways to allow an upgrade of systems already in the field not only with new algorithms, but also with new or enhanced credentials for entity authentication.

This paper is structured in the following way. Section II provides an overview about related work. Section III gives an overview on public key certificates and attribute certificates to show the general structure and approach. Section IV investigates a new approach utilizing attribute certificates to

 ISBN: 978-1-68558-099-5

support migration. Section V concludes the paper and provides an outlook to potential future work.

II. Related Work

The NIST challenge on replacement algorithms for digital signatures finishes after six years. Three digital signature candidates have been selected for standardization (see [10]):

- CRYSTALS-Dilithium
- FALCON
- SPHINCS+

These algorithms have different parameters and different parameter sizes as the classical algorithms like RSA or ECDSA. The key size can be significantly larger compared to classical cryptographic algorithms. This parameters and key sizes need to be supported by implementations and most importantly also in the context of existing user authentication credentials like X.509 certificates.

The migration or transition to quantum-safe cryptographic algorithms is a complex undertaking. The National Institute for Standards and Technology NIST has published a draft guideline on the migration to post-quantum cryptography [9].

Transition of cryptographic algorithms has been worked on in the context of ITU-T X.509 [1] with the support of alternative cryptographic algorithms as investigated in the following Section III.A.

With the IETF, a further standardization organization investigates into the different options of migration towards post-quantum cryptographic algorithms. Here the emphasis lies on utilizing hybrid approaches in protocols like TLS [2] or DTLS [3]. Besides integrating new algorithms in ciphersuites also approaches like Key Encapsulation (KEM, [11]) are being discussed to avoid generation of digital signatures on constraint devices.

III. Public Key and Attribute Certificates

X.509 certificates are used for entity authentication and integrity protection. As shown in Figure 1, the concept of a public key certificate is the binding of an entity's identity to a public key, which has a corresponding private key. This private key is kept secret by the entity and can be used to authenticate the entity. The certificate itself is issued by a trusted third party, a certification authority, that digitally signs the certificate. This signature is verified by the relying party as part of certificate path validation to a root certificate.

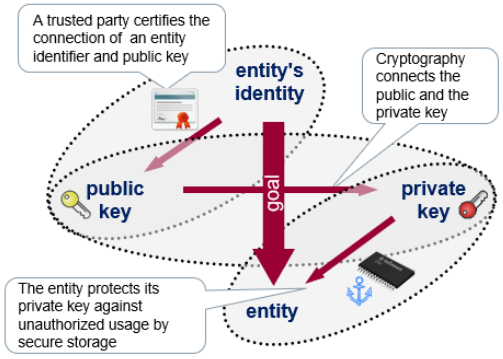

Figure 1. Concept of Binding Public Keys to Identities

These certificates are called public key certificates, as they bind the public key to an entity's identity. In addition, there attribute certificates are defined, which can be seen as temporary enhancement of public key certificates. They do not contain public keys but additional attributes that are connected to the holder of the public key certificate as shown in Figure 2. As visible in the figure, an attribute certificate has a validity period, which may vary based on the application use case. As the attribute certificate can be assumed as a temporary enhancement of a statements contained in a public key certificate, it may be short-lived or it may have a similar validity as the public key certificate. Figure 2 also shows that the issuing authority may be different for the attribute certificate as for the public key certificate. This fact may be interesting in cases where a separation of duty is targeted.

The following subsections will provide more details on both certificate types.

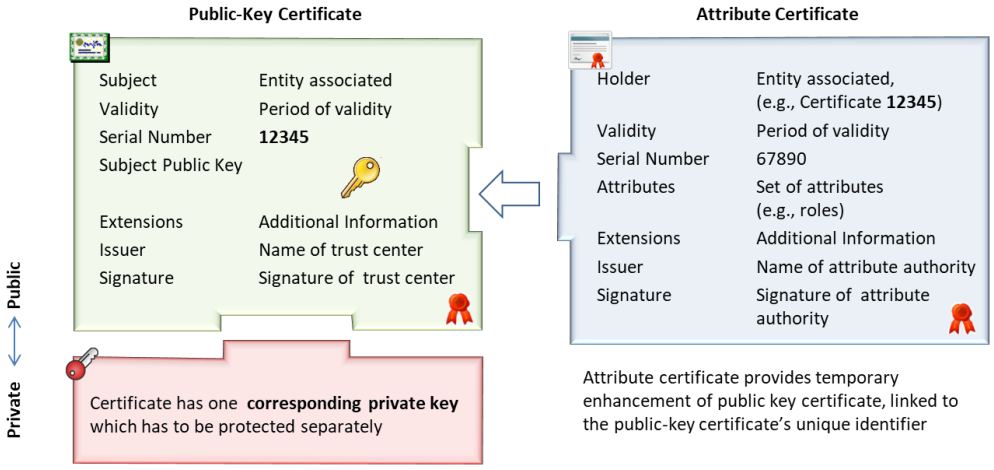

Figure 2. Concept of Public Key Certificates and Attribute Certificates

A. Public Key Certificates

ITU-T X.509 [1] is the public key certificate and attribute certificate framework widely applied in Information technology (IT) solutions an increasingly being used in Operational Technology (OT) solutions. It defines the structure and content of public key certificates as well as the verification of the components.

```
Certificate ::= SIGNED{TBSCertificate}

TBSCertificate ::= SEQUENCE {
  version                 [0]  Version DEFAULT v1,
  serialNumber                 CertificateSerialNumber,
  signature                    AlgorithmIdentifier{{SupportedAlgorithms}},
  issuer                       Name,
  validity                     Validity,
  subject                      Name,
  subjectPublicKeyInfo         SubjectPublicKeyInfo,
  issuerUniqueIdentifier  [1] IMPLICIT UniqueIdentifier OPTIONAL,
  ...,
  [[2:  -- if present, version shall be v2 or v3
  subjectUniqueIdentifier  [2] IMPLICIT UniqueIdentifier OPTIONAL]],
  [[3:  -- if present, version shall be v2 or v3
  extensions               [3]  Extensions OPTIONAL ]]
  -- If present, version shall be v3]]
} (CONSTRAINED BY { -- shall be DER encoded -- } )
```

Figure 3. Public Key Certificate structure (see [1])

As shown in Figure 3, the certificate is a signed structure, containing the `subject` as the name of the entity and the `subjectPublicKeyInfo` structure with information about algorithm and the contained public key. The certificate is signed by an issuing certificate authority. Besides further components the certificate structure can also be extended using the `extensions` component.

To support alternative algorithms, X.509 defines three extensions to convey the:

- `subjectAltPublicKeyInfo` – alternative public key
- `altSignatureAlgorithm` – alternative signature algorithm (used to sign the public key certificate) and
- `altSignatureValue` – alternative signature value.

Using theses extensions allows a relying party depending on its capabilities to either utilize classical cryptographic algorithms or alternative (here post quantum) algorithms for the verification of the certificate (and potential digital signatures performed with the public key corresponding to the contained public key. Depending on the security policy of the relying party, both signatures of the certificate may need to be verified.

This approach is limited to a single alternative key for a public key in practical application, i.e., limited to a single alternative cryptographic algorithm. Simply adding multiple alternative keys to the authentication certificate would increase the certificate size significantly.

B. Attribute Certificates

Besides public key certificates, ITU-T X.509 [1] also defines the structure and content of attribute certificates, as well as the binding to public key certificates and the verification of contained components. Note that besides the binding to public key certificates, an attribute certificate may also be bound to a name of an entity or some fingerprint of information.

An attribute certificate may be seen as temporary enhancement of a public key certificate.

```
AttributeCertificate ::= SIGNED{TBSAttributeCertificate}

TBSAttributeCertificate ::= SEQUENCE {
  version                 AttCertVersion, -- version is v2
  holder                  Holder,
  issuer                  AttCertIssuer,
  signature               AlgorithmIdentifier{{SupportedAlgorithms}},
  serialNumber            CertificateSerialNumber,
  attrCertValidityPeriod  AttCertValidityPeriod,
  attributes              SEQUENCE OF Attribute{{SupportedAttributes}},
  issuerUniqueID          UniqueIdentifier OPTIONAL,
  ...,
  ...,
  extensions              OPTIONAL }
```

Figure 4. Attribute Certificate structure (see [1])

As shown in Figure 4, similar to public key certificates an attribute certificate is also a signed structure, containing the `holder` as the name of the entity, information about the issuer, including the signature algorithm and values as well as the possibility to define extensions of the attribute certificate. Like for public key certificates, to support alternative algorithms, X.509 defines two extensions to convey the:

- `altSignatureAlgorithm` –alternative signature algorithm (used to sign the attribute certificate) and
- `altSignatureValue` – alternative signature value.

The standard does not foresee the capability to contain an alternative public key of the holder as additional attribute. The next section discusses the merits of providing this information as well as further, policy related information in the context of an attribute certificate.

IV. PROPOSED NEW ATTRIBUTES

As discussed in Section III, not all extensions defined for public key certificates are defined for inclusion in attribute certificates. This paper therefore proposes to use the `subjectAltPublicKeyInfo` extension also in attribute certificates to convey an alternative public key and information about the corresponding cryptographic algorithms, e.g., a public key for a post quantum asymmetric algorithm like FALCON, DILITHIUM, or SPHINCS+. This allows to associate and utilize alternative public keys to already existing certificates. As multiple attribute certificates can be issued for a single user certificate, implicitly various different cryptographic algorithms can be supported in a flexible way by issuing multiple corresponding attribute certificates.

Attribute certificates contain attributes, and providing an alternative public key as attribute is proposed as novel approach. It is intended to support smooth transition to public-key certificates using solely alternative, in the case here, post quantum cryptographic algorithms. As they are intended as temporary enhancement of public key certificates, this approach is seen appropriate. It is even possible to issue attribute certificates for an entity's public key certificate at a later point in time.

For migration to post-quantum cryptography, it is necessary to also support a security policy which handles the transition from one cryptographic algorithm to an alternative cryptographic algorithm (in the case here for digital signatures). Such a policy may require verifying only one signature, both signatures (classic and alternative), and may also provide a weight on the verification result, e.g., by the order of operations. Such a security policy may be configured

 ISBN: 978-1-68558-099-5

per relying party. In case of automation networks, it may be part of the engineering data for the Intelligent Electronic Devices (IED).

An alternative approach to the device configuration of security policies is the provisioning of the policy as part of the certificate, also in the form factor of an extensions. This paper proposes such an extension as shown in Figure 5 that may be applied in both certificate types, i.e., to public key certificates as well as to attribute certificates.

```
altCryptoPolicy ::= SEQUENCE {
  combAND     [0] boolean OPTIONAL,
  combOR      [1] boolean OPTIONAL,
  weightOnAlt [2] boolean OPTIONAL
}
```

Figure 5. Proposed Migration Policy Extension

The extension allows to specify the following security policies for the associated alternative public key:

- `combAND` requires the verification of the signature performed with the classic asymmetric algorithm as well as the alternative algorithm.
- `combOR` requires the verification signatures created with of either the classical or the alternative cryptographic algorithm,
- `weightOnAlt` indicates if the alternative algorithm has a higher weight in the evaluation. Note that this can be used in conjunction with `combOR` for the selection of classical or alternative signatures and also for the `combAND` case in cases, in which one signature verification may fail.

The extension may be included in the certificate as critical extension to ensure that it will be evaluated by the relying party. The inclusion into public key certificate can be done to associate a fixed security policy to the two contained public keys. There is also a benefit by placing the extension into an attribute certificate even in cases where the second public key is not contained in the attribute certificate but in the public key certificate. This approach allows to change the security without the need to issue a new public key certificate, enabling dynamic policy changes.

V. Conclusion and Outlook

This paper provides an overview on the need for a transition from currently used classical cryptographic algorithms to new, alternative cryptographic algorithms. More specifically, the focus is placed on the use of digital signatures and credentials conveying the public key within X.509 certificates.

In that respect, a novel approach for using alternative asymmetric algorithms in the context of these X.509 certificates has been described. It is proposed to support alternative public keys and associated information in attribute certificates, which enhances the application of already defined certificate extensions for public key certificates also for attribute certificates. By this approach, multiple cryptographic algorithms can be supported flexibly by issuing multiple attribute certificates corresponding to the different public keys of a user. Moreover, a further security policy extension is proposed that allows a dynamic adaptation of the security policy for the transition from classic cryptographic algorithms towards alternative, e.g., post quantum algorithms.

The discussed approach is currently in its infancy and needs to be implemented and tested to get practical experience. This is seen as the next consequent step. Due to the use of an already existing extension to transport the alternative public key, further investigation of the transport of algorithm specific parameters is not seen necessary as already considered in the originally defined extension.

Besides the necessity to perform more investigation of the side conditions of this approach and also a proof-of-concept implementation, it is seen necessary to also discuss this approach within standardization. This is due to the fact that most interacting systems are built with products from different manufacturers. Therefore, standardization is necessary to ensure interoperability of different manufacturers products.

References

[1] ITU-T X.509 ISO/IEC 9594-8:2020, Rec. ITU-T X.509 (2019), Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, https://www.itu.int/rec/T-REC-X.509-201910-I/en, [retrieved: August, 2023]

[2] E. Rescorla, IETF RFC 8446, “Transport Layer Security (TLS) Protocol v1.3”, August 2018, https://tools.ietf.org/html/rfc8446, [retrieved: August, 2023]

[3] E. Rescorla, H. Tschofenig, and N. Modadugu, IETF RFC 9147, “The Datagram Transport Layer Security (DTLS) Protocol Version 1.3”, April 2022 https://datatracker.ietf.org/doc/html/rfc9147, [retrieved: August, 2023]

[4] C. Kaufman, P. Hoffman, Y. Nir, P.Eronen, and T. Kirvinen., IETF RFC 7296, „Internet Key Exchange Protocol Version 2 (IKEv2)“, October 2014, https://datatracker.ietf.org/doc/html/rfc7296, [retrieved: August, 2023]

[5] B. Weis, S. Rowles, and T. Hardjono, IETF RFC 6407, “The Group Domain if Interpretation”, October 2011, https://datatracker.ietf.org/doc/html/rfc6407, [retrieved: August, 2023]

[6] A. J. Menezes, P. C. v. Oorschot, and S. A. Vanstone, “Handbook of Applied Cryptography”, CRC-Press, October 1996, ISBN: 0-8493-8523-7

[7] D. J. Bernstein, J. Buchmann, and E. Dahmen, “Post-quantum cryptography”, Springer, Berlin, 2009. ISBN 978-3-540-88701-0

[8] L. Cehen et al., NISTIR 8105, “Report on Post-Quantum Cryptography”, April 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf, [retrieved: August, 2023]

[9] W. Newhouse, M. Souppaya, W. Barker, and C. Brown, “Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography”, Volume A “Executive Summary”, NIST Special Publication 1800-38A, April 2023, https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms [retrieved: August, 2023]

[10] NIST Announcement, “PQC Standardization Process: Announcing Four Candidates to be Standardized”, July 2022, https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4, [retrieved: August, 2023]

[11] Giacon, F., Heuer, F., and B. Poettering, "KEM Combiners", January 2018, https://doi.org/10.1007/978-3-319-76578-5_7, [retrieved: August, 2023].

 ISBN: 978-1-68558-099-5