Decentralized Certificate Management for Network Function Virtualization (NFV) Implementation in 5G Networks

Junzhi Yan(✉), Bo Yang, Li Su, Shen He, and Ning Dong

China Mobile Research Institute, Beijing, China
{yanjunzhi,yangbo,suli,heshen,dongning}@chinamobile.com

Abstract. The certificate cost and certificate management complexity increase when PKI is leveraged into Network Function Virtualization (NFV), a significant enabling technology for 5G networks. The expected security of PKI cannot be met because the certificate revocation inquiry is unavailable during the intranet implementation in the operator's core network. This paper analyses the issues and challenges during the NFV implementation, and proposes a blockchain based decentralized NFV certificate management mechanism. During instantiation, the Virtual Network Functions (VNF) instance generates certificates according to the certificate profile provided in the VNF package. The certificates submitted to the decentralized certificate management system by the instance will be validated by corresponding participants. The certificates will be recorded into the ledger after validation and consensus, and then it will be trusted by the participants. The performance analysis shows the transaction efficiency is non-critical, and the transaction delay of seconds is acceptable in this decentralized system. The delay of the certificate inquiry is critical, and it can be fulfilled by the decentralized deployment of inquiry nodes.

Keywords: Blockchain · NFV · Certificate management · PKI

1 Introduction

Network Function Virtualization (NFV), featured as decoupling software from hardware, flexible network function deployment, and dynamic operation, is a significant enabling technology for 5G networks. In NFV, network functions are implemented by vendors in software components known as Virtual Network Functions (VNFs), which are deployed on cloud infrastructure or massively distributed servers instead of dedicated hardware [1].

The architectural framework of NFV defined by the European Telecommunication Standardization Institute (ETSI) is depicted in Fig. 1. It enabled the execution and deployment of VNF on NFV infrastructure comprising a pool of network, storage, and computing resources. The NFV infrastructure is usually a decentralized cloud infrastructure

J. Xiong et al. (Eds.): MobiMedia 2021, LNICST 394, pp. 81–93, 2021.
https://doi.org/10.1007/978-3-030-89814-4_6

in which servers are distributed over various locations. ETSI defines network functions, including VNFs. The operation, deployment, and execution of network services and VNFs in NFV infrastructure are controlled by an orchestration and management system, whose performance is steered by NFV descriptors [1, 2].

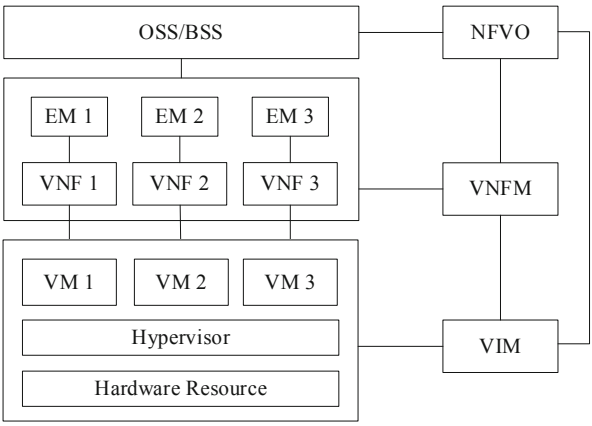

Fig. 1. Architectural framework of NFV defined by ETSI [2]

Typically, NFV is capable of overcoming certain 5G challenges, such as, reducing the energy cost by maximizing the resource usage, scaling and mobilizing VNFs from one resource to another, ensuring VNFs performance operations [3]. A VNF is a virtualisation of a network function in a legacy non-virtualised network. In 5G networks, Network Functions (NFs) are defined in 3GPP TS 23.501 [4].

PKI certificates are widely used by the VNF, MANO (Management and Orchestration), OSS/BSS/EM (Operation Support Systems, Business Support System, Element Management) in NFV. These certificates are used for authentication and secure communication. The NFs in 5G networks use TLS protocol to connect each other [5]. However, some issues and challenges arise during the deployment of the NFV. These issues and challenges are related with the certificate cost, across-domain trust, CRL/OCSP (Certificate Revocation List/Online Certificate Status Protocol) services, certificate validation and certificate maintenance. The essence of some issues is the lack of trust amongst the multiple participants in the NFV deployment. Blockchain featured as decentralization and tamper resistant may benefit PKI technology [6]. The blockchain based decentralized PKI is a significant trend for PKI technology [7], which could be used to facilitate the certificate management of NFV.

The main contribution of this paper is the blockchain based decentralized NFV certificate management system, which aims to solve the issues in NFV implementation in telecommunication operator's network. Section 2 discusses the related researches. The issues and challenges aroused during the NFV implementation is discussed in Sect. 3. Section 4 provides the framework of decentralized NFV certificate management mechanism, and the certificate management method. The performance is analyzed in Sect. 5. The conclusion is in Sect. 6.

2 Related Works

ETSI has published series of NFV standards, of which ETSI GS NFV 002 defines the architectural framework [2], ETSI GS NFV 001 [8] provides a list of use cases and examples of target network functions for virtualization,ETSI GR NFV SEC 005 [9] analyses the certificate management using traditional PKI.

An overview of enabling technologies like NFV and SDN for 5G was provided in [10]. It described the 5G slicing notion and the prominent challenges associated with it, and highlighted a few challenges for ensuring an envisaged 5G networking system.

The concept of Network Slicing (NS) as a service was presented for providing customized services in [11]. An outline of sophisticated standardization views of NS was provided in [12]. There are crucial challenges in NS faced by telecommunication operators such as difficulties in attaining end-to-end NS, stable migration, interoperability, and roaming. The work highlighted that base station virtualization and wireless resource sharing to formulate appropriate requirements and create standardized slices should be emphasized. 5G architecture design was presented for NS and building NFV, Software Defined Network (SDN) technologies in [13]. It emphasized schemes which provide effective substrate resource utilization for NS. In [14], the performance deterioration issue of virtualized access points occurring due to NFV implementation was addressed and an overcoming approach was presented. In [15], a framework for mobile network virtualization comprising three planes, namely control, cognitive, and data planes, was presented. A blockchain-based secure key management scheme was proposed in [16] to address the security of key management caused by a non-trusted base station, it was suited to improve the trustworthiness of the base station. The incentive mechanism combining edge computing was addressed in [17].

Some typical researches focusing on the decentralized PKI could be found in [7, 18–22]. A blockchain based PKI framework in mobile networks was proposed in [7]. It focused on the problems when traditional PKI is leveraged into mobile networks. The system was constituted by submission nodes, validator nodes, inquiry nodes. It provided some scenarios and application cases in mobile networks. The optimizations for certificate storage in blockchain based PKI system was analyzed in [18]. The provided methods aimed to improve the storage efficiency of specific nodes in blockchain based PKI system. Research in [19] focused on the trust among multiple CAs using blockchain, and provided some use cases in mobile networks.

The implementation of Yakubov et al. [20] used the standard X.509v3 certificate with an addition to the extension fields to indicate its location in the blockchain. The smart contract of each CA contained one list with all issued certificates and another list for revoked certificates. BlockPKI [21] required multiple CAs to perform a complete domain validation from different vantage points for an increased resilience to compromise and hijacking, scale to a high number of CAs by using an efficient multi-signature scheme, and provided a framework for paying multiple CAs automatically. SCPKI [22] worked on Ethereum blockchain, and used an entity or authority in the system to verify another entity's identity. It could be used to detect rogue certificates when they are published.

Standard development organizations such as ISO/IEC, ITU-T have begun to study and standardize blockchain based PKI and certificate management technology. These works are focusing on the profile and the mechanism of blockchain recorded certificates. However, these normative works are still under development.

3 Issues and Challenges

In NFV, there are mainly three kinds of use cases for the use of certificates [9], i.e., VNF certificate use case, MANO certificate use case, and OSS/BSS/EM certificate use case. The VNF certificate use case will be discussed in this paper. The other two use cases are similar.

A VNF component instance (VNFCI) needs one or more certificates provisioned to attest its identity to the VNFM or EM to establish a secure connection between them. In NFV implementation, the number of VNF certificates is far more than that in the other two use cases. The management of VNF certificates will be discussed in this paper. However, the certificates in the other two use cases could use the same method as VNF certificates.

By using traditional solutions, each instance of VNF could enroll certificates to CA/RA directly, or by a delegator such as VNFM [9]. However, the issues and challenges are as follows:

- Cost of certificates

  VNFs are implemented with one or more VNF components. While a VNF component instance composed of various VNFCIs could have multiple logical identities, each of which is represented by a certificate, to communicate with different peers [9]. As a result, there will be a huge number of certificates required for the VNFs in 5G networks. It will be costly to use certificates issued by commercial CAs. The telecommunication operators prefer to use their own CA, vendor's CA or designated CA to provide certificate service due to the cost. This may cause the problem of trust across CA domains.
- Trust across CA domains

  A VNFCI may communicate with another VNFCI in another telecommunication operator's network. These two VNFCIs may be configured with the certificates issued by different CAs. There are several traditional methods to deal with multiple CAs, including trusted root list, cross certification, bridge CA, each with its own pros and cons as illustrated as following.

  – Trusted root list: It relies on the list maintained by the relying party. Certificates issued by the roots which are not in the list will not be trusted. It will be costly to update the list.
  – Cross certification: It's suitable for a small amount of CAs. If there are a large amount of CAs, the cross relationship will make a complex structure. Moreover, the usage of certificate policies will be limited after multiple mappings.
  – Bridge CA: The bridge CA will connect multiple CAs. The certificate chain would be longer, and the validation would be much more complex and expensive.

- CRL/OCSP unavailable due to intranet implementation

  The 5G network functions are deployed in the telecommunication operator's core network with no connection to the Internet, which means CRL/OCSP are unavailable. Moreover, the telecommunication operator's core network is usually divided into different security domains. These security domains are isolated physically or logically. The entity in one security domain cannot communicate with the entities in another security domain directly. In practice, the telecommunication operator's CA/RA service, including CRL/OCSP services, are implemented in different security domains from the 5G NFs in the core network. This means the VNFCIs in the 5G core network cannot access the CRL/OCSP services provided by the telecommunication operator's CA. Unless, the telecommunication operator deploys the CRL/OCSP services in each security domain, which is a complex and costly work.
- Certificate validation

  Before a VNFCI gets a certificate issued by the CA/RA, the VNFCI will be validated by the CA/RA. The subject field in the certificate may be an IP address, FQDN, or other unique identifiers, and these information is related with the deployment. One VNFCI could have several functionalities and several logical interfaces, and it could have several identities for different functionalities and interfaces. It is impossible for the CA/RA to validate the subject field, since the CA/RA does not get the information related with the deployment or the identities of the VNFCI. In practice, these is an endorsement for the subject field. The endorsement is provided by some designated administrators. In accordance with the use cases, there will be kinds of certificates endorsed by different administrators. In such case, the deep cooperation between the CA/RA and the administrators is significant and it makes the certificate management complicated.
- Certificate maintenance

  Each certificate has a validation period, which means it may expire. The certificate to be expired needs to be renewed. Or else it will not be trusted by the relying party. There was once some mobile service became unavailable because of the expired certificates. In 5G networks, there will be more than thousands of VNF certificates. It has to be ensured each certificate be renewed before it expires, and be revoked when it is insecure or the VNFCI is terminated. In practice, the certificate renew could be optional, since the VNFCI with an expired certificate could be terminated, and a new VNFCI could be instantiated with a new certificate.

  The essence of the above issues is the lack of trust amongst the multiple participants (such as vendors, administrators of the telecommunication operator, CA/RAs) during the NFV implementation. A secured information sharing and trusted endorsement method is necessary to solve the issues. The blockchain is featured as decentralization and tamper-resistant. The endorsement and consensus mechanisms in blockchain help to make the information submitted to the participants in the blockchain system be trusted. It provides a decentralized way to solve the issues of the NFV certificate management.

4 Decentralized NFV Certificate Management

4.1 Framework

A blockchain based PKI framework was proposed in [7]. It consists submission nodes, validator nodes, and inquiry nodes, while the submission node is used to submit certificates to the blockchain based PKI system, the validator node is the node to verify the received requests and generate new blocks, and the inquiry node works to provide certificate and status inquiry service. In this VNF certificate management scenario, the framework for VNF certificate management is shown in Fig. 2.

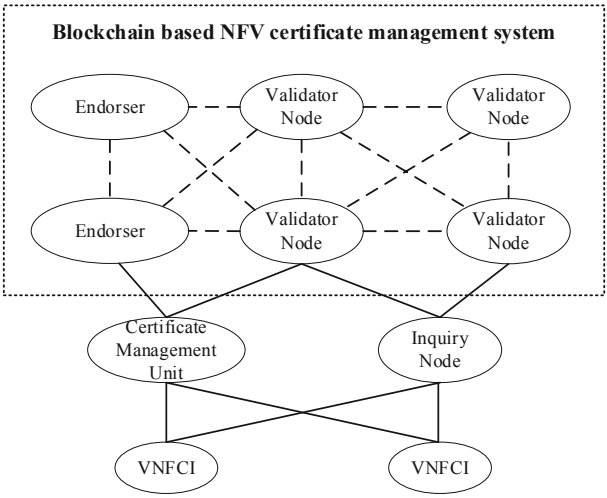

Fig. 2. Framework for decentralized NFV certificate management system

The VNFCI is the owner of the certificate.

The Certificate Management Unit (CMU) works as a client to submit certificates and related information into the blockchain based NFV certificate management system. The CMU could be a function in NFV architecture, e.g., located in VNFM, and it also could be independent to the NFV architecture.

The endorser is the node to endorse the identity in the submitted certificates. Only the endorsed certificates and requests could be processed by the validator nodes.

The validator node is the node to verify the received requests and generate new blocks. It validates the certificates and request according to the policies. The validator nodes are held by vendors, operators, and CAs. One node could act as both an endorser and a validator.

The inquiry node provides certificate inquiry services. It needs to receive new blocks, but do not need to participate into the generation of new blocks. The inquiry nodes are held and deployed by any party which is capable to access the blockchain based certificate management system.

4.2 Certificate Enrollment

During instantiation, VNFCI needs to enroll certificates to communicate with other VNFCI or MANO/OSS/BSS/EM. The certificate could be a certificate issued by CA/RA as descripted in [9]. It could also be a self-signed certificate generated by the VNFCI. The self-signed certificate management will be discussed in this paper. The certificate profile is provided to the VNFCI during the VNF configuration. While the management of certificates issued by traditional CAs is also supported, which is similar to the self-signed certificates.

The VNF configuration is based on parameterization captured at design time, included in the VNF package, and complemented during the VNF instantiation. Before a VNF is installed, the VNF package will be on-boarded by NFVO. The VNF package includes a component of VNFD (Virtualised Network Function Descriptor), which is a deployment template describing a VNF in terms of deployment and operational behavior requirements [23]. The VNFM accesses to the VNFD, and configures the certificate profile during the VNF instantiation. The VNFCI enrolls a certificate as follows and the message flow is shown in Fig. 3.

0. The VNFM generates the certificate profile and initial credential for each VNFCI which are included in the VNFD, sends the certificate profile and token for each VNFCI to the CMU.

The VNF parameters describing the certificate profile in the VNFD can be declared to be configurable during the VNF design phase, and further be configured by the VNFM during or after the VNF instantiation [24]. The certificate profile declares the information used to generate the certificate, such as the subject, key usage, basic constraint [7, 25].

The subject field identifies the entity associated with the public key stored in the subject public key field, and contains a distinguished name. The distinguished name may be an FQDN, a serial number, or other kinds of names, according to the operator's policy. It is suggested to include the operator's information in the distinguished name field, so as to identify the HPLMN (Home Public Land Mobile Network) in roaming scenarios. Multiply names could be addressed in the SAN (Subject Alternative Name) field [25]. The address of the inquiry node could be included in the extension field of the certificate.

The VNFM sends the certificate profile and a token to CMU. The token and information in the certificate profile will be used to validate the submitted VNFCI certificates. For the sake of simplicity, we use a token which is the value of multiple hash operations on the initial credential. The initial credential is kept as a secret by the VNFCI. Denote the initial credential by x, the token by y. Then we have

$$\mathrm{H}\left(\mathrm{H}(\ldots \mathrm{H}(x))\right) = y \tag{1}$$

y is the value of multiple times (e.g., n times) hash operations of x.

1. The VNFCI generates a self-signed certificate, and submits the certificate publish request to the CMU.

The public-private key pair used to generate a self-signed certificate is generated using the methods addressed in [9]. The VNFCI generates the certificate using the information and certificate profile provided in the VNFD, and then generates the authentication credential based on the initial credential. The authentication credential is the value (denoted by y_1) of multiple hash operations (e.g., n-1 times) on the initial credential (x), of which the hash value equals the token (y). The VNFCI submits certificate publish request to the CMU, while the request consists the certificate and the authentication credential.

Message flows for VNFCI certificate enrollment:

0. VNFM: Configures the certificate profile in VNFD, generates an initial credential and a token
   VNFM → VNFCI:
   {certificate profile, initial credential x}
   VNFM → CMU:
   {certificate profile, token y}

1. VNFCI: Generates a certificate using the certificate profile
   VNFCI → CMU: certificate publish request
   {certificate, authentication credential y_1}

2. CMU: verifies and signs the request, update the token
   The identity in the certificate is correct
   Authentication credential is valid, update the token into y_1
   CMU → Blockchain based system: certificate publish request
   {certificate, signature}

3. Endorsers: verify the request
   Signature is correct
   Validator nodes: record the certificate and status into a newly generated block after consensus

Fig. 3. Message flows for VNFCI certificate enrollment

2. The CMU verifies the certificate publish request, signs the request and transmits it to the blockchain based certificate management system.

The CMU verifies the certificate in the request to ensure it is consistent with the certificate profile, and the information contained in the certificate is correct (e.g., the information in the subject field is valid). The authentication credential is verified to ensure it is consistent with the token. Then the CMU signs the request and submits it to the blockchain based certificate management system. The token could only be used once so as to prevent replay attacks. Thus, CMU updates the token from y into y_1. The one-time token makes it possible for the VNFCI to enroll multiple certificates.

3. The endorsers in the blockchain system verifies the request, endorses the verified request. The certificate in the endorsed request will be recorded into the ledger by the validator nodes.

The endorsers verify the signature of the certificate publish request. After verification, the endorsers sign the request with their private keys. The validator nodes record the certificates in the endorsed requests into the ledger after consensus. The endorsement policy is made and configured by the participants.

4.3 Certificate Revocation

A VNFCI certificate needs to be revoked, when it is insecure or the VNFCI is terminated. At first, the VNFCI generates and submits a certificate revocation request to the CMU. Or, the CMU generates the certificate revocation request according to the policy. The request contains the certificate or its identifier, and then it is signed by the CMU.

The CMU submits the certificate revocation request to the blockchain based certificate management system. The endorsers and validator nodes verify the request and then update the status of the certificate as "revoked" in the ledger.

4.4 Certificate Renewal

The certificate to be expired needs to be renewed. The certificate renewal request is initiated by the VNFCI. The CMU could indicate the VNFCI to initiate a certificate renewal process.

The VNFCI generates the certificate renewal request and submits it to the CMU. The request contains the certificate to be renewed or its identifier, the new certificate, and the signature signed by the private key corresponding to the certificate to be renewed. The CMU submits the certificate renewal request to the blockchain based certificate management system. The endorsers and validator nodes verify the request and then record the new certificate into the ledge, and update the status of the former certificate as "revoked" in the ledger.

4.5 Certificate Inquiry

Ideally, the NFV infrustructure of all the telecommunication operators use the blockchain based certificate management solution. However, in practice, some operators may use blockchain based solution while others use traditional PKI solution. The certificate inquiry is discussed as follows in non-roaming scenario and roaming scenario, in which the VPLMN (Visited Public Land Mobile Network) uses the blockchain based solution.

1. Non-roaming scenario
   When a VNFCI receives a certificate from another VNFCI, it inquires the certificate and its status from the inquiry node of the blockchain based certificate management system, the inquiry node finds the inquired certificate and its status, and feedbacks them to the relying party. The relying party verifies the certificate and its status to ensure the certificate is valid.

2. Roaming scenario
   Figure 4 depicts a simplified certificate inquiry architecture in the case of local break out scenario which was defined in [4]. It shows an example of local break out scenario. Usually, each operator only trusts its own system, including the NFV certificate management system. In this case, the VPLMN uses the blockchain based solution, HPLMN 1 uses the traditional PKI solution, and HPLMN 2 uses the blockchain based solution which is independent to the VPLMN.

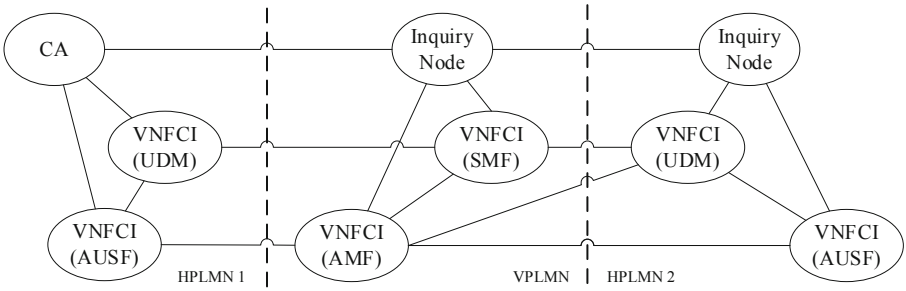

Fig. 4. Certificate inquiry architecture for roaming 5G system

The inquiry node in the VPLMN connects the CRL/OCSP servers used by HPLMN 1, and the inquiry node in NFV certificate management system of HPLMN 2. When a VNFCI in the VPLMN receives a certificate from the VNFCI of other PLMN, it connects the inquiry node in VPLMN for the status of the certificate. The certificate in this blockchain based solution contains the operator's information or the address of the inquiry node. The certificate in the traditional PKI solution contains the CRL/OCSP address. As a result, the inquiry node in the VPLMN connects the CRL/OCSP server in HPLMN 1, and the inquiry node in HPLMN 2, according to the information included in the certificate. The inquiry node in the VPLMN inquiries the certificate status and feedback the status to the VNFCI in the VPLMN.

5 Performance Consideration

5.1 Transaction Efficiency of Certificate Management

The certificate management requests including certificate enrollment, renewal and revocation are blockchain transactions, which means the transaction validation is needed and new blocks are generated. Transaction throughput, which is the number of transactions could be processed in a given time period, determines the efficiency of a blockchain based system. High transaction throughput means more requests could be processed in a given time period.

In NFV scenario, the certificate enrollment happens during instantiation. It happens once or no more than several times for each VNFCI. Usually, the validity of a certificate

is 1-year long. However, it could be configured according to the operator's policy. The longer is the validity, the less certificate renewal is needed. Each certificate can only be revoked once. As a result, the certificate for each VNFCI needs no more than two transactions (certificate enrollment/renewal, and certificate revocation) per year on average. Even if there are millions of VNFCIs in the operator's network, about tens of transactions happen per minute. The transaction efficiency is non-critical in this decentralized system.

5.2 Transaction Delay

Each certificate management request may result in a new record in the ledger. Transaction delay means the time from the certificate management request submitted to the blockchain based system to the time that the request be processed and recorded into a new block or be rejected. It usually takes minutes to instantiate a VNFCI, so the transaction delay of seconds is acceptable. The most commonly used blockchain framework such as Fabric and Etherum support the transaction delay of seconds. Both of them could be used to implement the decentralized NFV certificate management system.

5.3 Performance of Certificate Inquiry

In the traditional PKI system, the certificate status is inquired by using CRL or OCSP, which is centralized service provided by CA. In blockchain based NFV certificate management system, each node capable to access the ledger could provide certificate status inquiry service. This makes the inquiry service be decentralized. When an inquiry node is deployed on the edge of the operator's core network and Internet, it could provide local certificate inquiry service for the entities in the core network. This may greatly enhance the availability and efficiency of certificate status inquiry service.

5.4 Other Considerations

Some other considerations about the cost, trust across domains, compatibility are as follows:

- Cost: There is no need for the operator and vendor to deploy and maintain a CA infrastructure for the NFV implementation, so the cost is reduced.
- Trust across domains: The nodes in the decentralized system consist operators, vendors, traditional CAs, which may be from different trust domains. The endorsement and consensus mechanisms make all the records in the ledger be trusted by the multiple participants from different domains according to the policy. It makes the trust between different trust domains be available.
- Compatibility: X.509v3 certificate [26] is supported in blockchain based certificate management system, so as to be compatible with the traditional PKI system and applications.

6 Conclusion

Decentralized PKI is a significant direction for PKI technology. This paper analyses the issues and challenges related to the certificate management aroused during the NFV implementation in the 5G networks, and proposes a blockchain based decentralized NFV certificate management mechanism. The system could establish the trust among the participants in the NFV implementation, such as vendors, operators, even traditional CAs. It could ease the work load of the certificate management, reduce the cost to deploy and maintain the CA, and make certificate status inquiry available in the 5G core network. The analysis shows that the performance of transaction efficiency is non-critical in the blockchain based decentralized system. The high performance of the certificate inquiry could be facilitated by the decentralized deployment of inquiry nodes. This work could also facilitate the certificate usage in other scenarios in the telecommunication operator's networks.

References

1. Srinivasan, S.: A literature review of network function virtualization (NFV) in 5G networks. Int. J. Comput. Trends Technol. **68**(10), 49–55 (2020)
2. ETSI GS NFV 002: Network Functions Virtualisation (NFV); Architectural Framework (2014)
3. Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., et al.: Network slicing for 5G with SDN/NFV: concepts, architectures, and challenges. IEEE Commun. Mag. **55**(5), 80–87 (2017)
4. 3GPP TS 23.501: System Architecture for the 5G System (2019)
5. 3GPP TS 33.501: Security architecture and procedures for 5G system (2019)
6. Hepp, T., Spaeh, F., Schoenhals, A., et al.: Exploring potentials and challenges of blockchain-based public key infrastructures. In: 2019 IEEE Conference on Computer Communications Workshops (IEEE INFOCOM 2019), pp. 847–852. IEEE (2019)
7. Yan, J., Hang, X., Yang, B., et al.: Blockchain based PKI and certificates management in mobile networks. In: IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2020), Los Alamitos, California, pp. 1764–1770. IEEE Computer Society (2021)
8. ETSI GS NFV 001: Network Functions Virtualisation (NFV); Use Cases (2013).
9. ETSI GR NFV-SEC 005: Network Functions Virtualisation (NFV); Trust; Report on Certificate Management (2019)
10. Yousaf, F.Z., Bredel, M., Schaller, S., Schneider, F.: NFV and SDN—Key technology enablers for 5G networks. IEEE J. Sel. Areas Commun. **35**(11), 2468–2478 (2017)
11. Zhou, X., Li, R., Chen, T., et al.: Network slicing as a service: enabling enterprises' own software-defined cellular networks. IEEE Commun. Mag. **54**(7), 146–153 (2016)
12. Kim, D., Kim, S.: Network slicing as enablers for 5G services: state of the art and challenges for the mobile industry. Telecommun. Syst. **71**(3), 517–527 (2019)
13. Yousaf, F.Z., Gramaglia, M., Friderikos, et al.: Network slicing with flexible mobility and QoS/QoE support for 5G networks. In: IEEE International Conference on Communications Workshops (ICC Workshops 2017), pp. 1195–1201. IEEE (2017)
14. Wang, X., Xu, C., Zhao, G., et al.: Tuna: an efficient and practical scheme for wireless access points in 5G networks virtualization. IEEE Commun. Lett. **22**(4), 748–751 (2017)
15. Feng, Z., Qiu, C., Feng, Z., et al.: An effective approach to 5G: wireless network virtualization. IEEE Commun. Mag. **53**(12), 53–59 (2015)

16. Tian, Y., Wang, Z., Xiong, J., et al.: A blockchain-based secure key management scheme with trustworthiness in DWSNs. IEEE Trans. Industr. Inf. **16**(9), 6193–6202 (2020)
17. Xiong, J., Chen, X., Yang, Q., et al.: A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing. IEEE Trans. Network Sci. Eng. **7**(4), 2347–2360 (2020)
18. Yan, J., Yang, B., Su, L., He, S.: Storage optimization for certificates in blockchain based PKI system. In: Xu, Ke., Zhu, J., Song, X., Lu, Z. (eds.) CBCC 2020. CCIS, vol. 1305, pp. 116–125. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-6478-3_8
19. Yan, J., Peng, J., Zuo, M., et al.: Blockchain based PKI certificate system. Telecom Eng. Tech. Stand. **2017**(11), 16–20 (2017)
20. Yakubov, A., Shbair, W.M., Wallbom, A., et al.: A blockchain-based PKI management framework. In: 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS 2018), pp. 1–6. IEEE (2018)
21. Dykcik, L., Chuat, L., Szalachowski, P., et al.: BlockPKI: an automated, resilient, and transparent public-key infrastructure. In: 2018 IEEE International Conference on Data Mining Workshops (ICDMW 2018), pp. 105–114. IEEE (2018)
22. Al-Bassam, M.: SCPKI: A smart contract based PKI and identity system. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, pp. 35–40. ACM (2017)
23. ETSI GS NFV-IFA 011: network functions virtualisation (NFV) release 4; management and orchestration; VNF descriptor and packaging specification, (2020)
24. ETSI GS NFV-IFA 008: network functions virtualisation (NFV); management and orchestration; Ve-Vnfm reference point - interface and information model specification (2019)
25. IETF RFC 5280: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile (2008)
26. ITU-T X.509. The directory: public-key and attribute certificate frameworks (2016)