**3GPP TSG-SA3 Meeting #105 *S3-213884***

**e-meeting, 08 - 19 Nov 2021 draft\_S3-213884-r2**

**Source: MITRE**

**Title: New solution: Ticket based access control for administrators**

**Document for: Approval**

**Agenda Item: 5.3**

1 Decision/action requested

***This pCR proposes to solve Key Issue #10 and 22***

2 References

[1] 3GPP TR 33.848 " Study on Security Impacts of Virtualisation".

[2] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[3] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, DOI 10.17487/RFC4120, July 2005, <https://www.rfc-editor.org/info/rfc4120>.

[4] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

3 Rationale

Administrators (“admins”) have many responsibilities within the NFV environment, such as starting/stopping VNF instances, ensuring resources are provided to the VNF, and orchestrating the NFV. These responsibilities should only be given to privileged admins. If the admins account is compromised or the admin is malicious then the account can be used to perform nefarious attacks on the NFV (e.g., espionage, selling user data, service disruption). To reduce the risk of a malicious admin or MANO single point of failure the principles highlighted in Annex A. and Solution #3 should be followed.

To that end, this solution proposes using a ticket-based authentication system and Attribute Based Access Control (ABAC) on the NFV management plane. Within ETSI GS NFV-SEC 003 [2] it suggests *a token-based authentication mechanism such as Kerberos may be used between the Tenant Domain and Infrastructure Domain*. A token-based authorization framework that can be used is OAuth 2.0, specified in IETF RFC 6749 [4]. Similarly, this Kerberos solution uses an authentication server to authenticate the admin. Next, a ticket granting server issues a ticket to authenticated admins which is used to connect securely to an NFV component. Tickets issued should be restricted by both time and number of usages. The admin uses the ticket to securely connect to the VNF or NFVI and perform necessary MANO functions. All other connection requests to the NFV environment shall be denied.

Once, the admin is authenticated and has established a secure connection with the NFV environment, they must also be authorized to perform tasks. ABAC may be used to provide fine grain access control to resources within the NFVI or the VNFs. ABAC uses policies that are based on subject attributes (e.g., user, admin, senior admin), object attributes (e.g., VNF, NFVI), and environmental conditions (e.g., time, location, authentication strength). Such attribute based policies help protect the NFV environment from unusual/ suspicious behaviour, even when the source is authenticated. Together, ticket-based authentication and ABAC provide secure access to the NFV resources, and fine grain access control.

4 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.848.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.XX Solution #XX: Ticket-based access control for NFV

### 6.XX.1 Introduction

This solution aims to provide one approach to address KI 10: Single Administrator Domain, and KI 22: MANO Single Point of Failures.

Administrators (“admins”) have many responsibilities in the NFV such as starting/stopping VNF instances, ensuring resources are provided to the VNF, and orchestrating the NFV infrastructure. These responsibilities should only be given to privileged admins. If the admin account is compromised or the admin is malicious then the account can be used to conduct attacks on the NFV (e.g., data exfiltration/espionage, selling user data, unauthorized configuration or package modification, service disruption). To reduce the risk of a malicious admin or MANO single point of failure the principles highlighted in Annex A. and Solution #3 must be followed.

To that end, this solution proposes using a ticket-based authentication system and Attribute Based Access Control (ABAC) on the NFV management plane. Within ETSI GS NFV-SEC 003 [2] it suggests *a token-based authentication mechanism such as Kerberos may be used between the Tenant Domain and Infrastructure Domain*. Similarly, this solution uses an Authentication Server (AS) to authenticate the admin. Next, a Ticket Granting Server (TGS) issues a ticket to authenticated admins which is used to connect securely to an NFV component. Tickets issued should be restricted by both time and number of usages. All other connection requests to the NFV environment shall be denied.

Another token-based authorization framework that can be used is OAuth 2.0, specified in IETF RFC 6749 [4]. Herein we only give details for the Kerberos option.

Once, the admin is authenticated and has established a secure connection with the NFV environment, they must also be authorized to perform tasks. ABAC may be used to provide fine grain access control to resources within the NFVI or the VNFs. ABAC uses policies that are based on subject attributes (e.g., user, admin, senior admin), object attributes (e.g., VNF, NFVI), and environmental conditions (e.g., time, location, authentication strength). Such attribute based policies help protect the NFV environment from unusual/ suspicious behaviour, even when the source is authenticated. Together, ticket-based authentication and ABAC provide secure access to the NFV resources, and fine grain access control.

### 6.XX.2 Solution details

To implement necessary access controls, this solution proposes using a ticket-based authentication mechanism and ABAC. Kerberos, described in IETF RFC 4120 [3], is a network authentication protocol that uses tickets to authenticate a client’s connection to a server. It uses shared secret key cryptography to provide a secure connection between the client, Key Distribution Center (KDC), and server.

In this solution, a ticket-based authentication protocol, like Kerberos, is used to authenticate admins attempting to gain access to the NFV resources (VNF or the NFVI). In this case the client is an admin requesting access to the NFV environment. Additionally, ABAC is used on the resource side to authorize the admin. The ABAC server is per domain (VNF or NFVI) and implemented in such a way as to not be a single point of failure (e.g., distributed or redundant). The procedure for admin authentication and authorization to perform Management and Orchestration (MANO) functions is depicted in figure 6.XX.2.1.

We note that the VNFs themselves and the infrastructure they run on (NFVI) can and should be two different administrative domains. The KDC can be per domain or can serve several domains. A policy server can be a part of the KDC and handles access control for each domain.

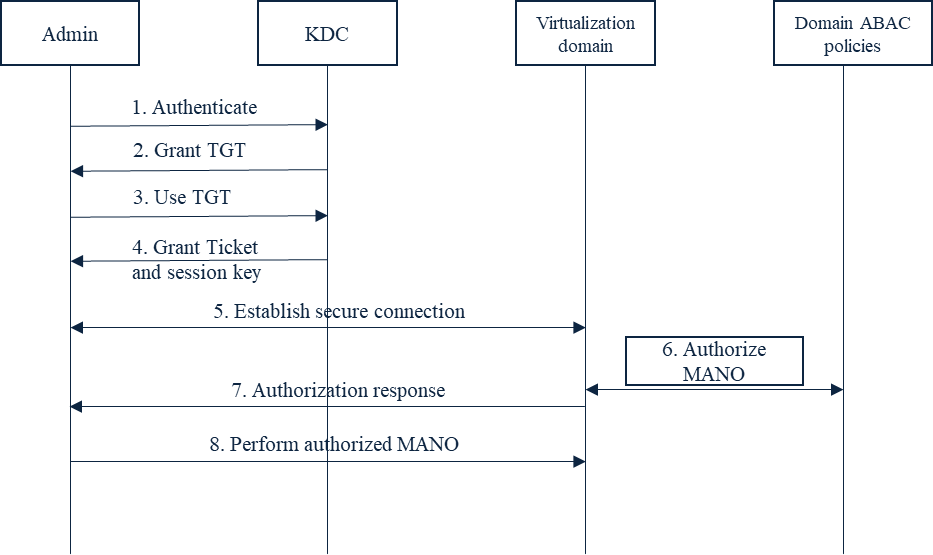


Figure 6.XX.2.1: Procedure for admin authentication and authorization to perform Management and Orchestration (MANO) functions, applicable for each of the domains: NFVI and VNF.

Step 1: The admin sends an authentication request to the Authentication Server (AS) that is part of the Key Distribution Center (KDC).

Editor’s note: It is FFS whether the interaction between the Admin and the KDC is in scope of 3GPP.

Step 2: Upon successful authentication the KDC issues a Ticket Granting Ticket (TGT) to the admin.

Step 3: The admin sends the TGT to the Ticket Granting Service (TGS) that is part of the KDC to request access to the resource (NFVI/VNF).

Step 4: If access is approved, the KDC sends the admin a session key and ticket to access the resource (NFVI/VNF). If the KDC limits the number of access attempts, then the remaining access attempts should be decreased by one every time a ticket is issued.

Step 5: Once authenticated and authorized by the KDC, the admin can send the ticket with the session key to the resource (NFVI/VNF). Admin can use the session key to communicate securely with the resource (NFVI/VNF) for the duration of time on the ticket.

Editor’s note: It is FFS whether the interaction between the Admin and the NFVI or the VNF is in scope of 3GPP.

Step 6: The resource (NFVI/VNF) sends an authorization request to the ABAC server on behalf of the admin. The ABAC server may be co-located with the resource (NFVI/VNF), but access must only be granted to authorized admins with the highest privileges. The ABAC server grants authorization using attribute based rules (e.g., admin A is allowed access to resource B from IP address: 1.2.3.4 from 9:00-10:00 UTC).

Step 7: The resource (NFVI/VNF) sends an authorization response. If the admin is unauthorized to perform the requested MANO functions, then the resource drops the connection.

Step 8: The admin performs the authorized MANO functions.

Step 9: Once the allotted time on the Ticket is reached, the resource (NFVI/VNF) drops the connection with the admin.

### 6.XX.3 Evaluation

.TBD

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*