**3GPP TSG- Meeting # *S4-240920***

**,**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **Pseudo CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **-** | **Current version:** | **4** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | : Extending 5GMS with Oauth 2.0 support | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GMS\_Pro\_Ph2 | | | | |  | ***Date:*** | | | 03.11.2023 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The OpenAPI definitions within TS 26.510 are extended for the usage of Oauth 2.0 (according to the SA3 guidelines) for 5GMS protocols based on the conclusions in TR 26.804, clause 6.9. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex C.3, Annex C.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | |  | | |
| ***affected:*** | |  |  | Test specifications | | | |  | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | |  | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev 01:   * Add OAuth Client Credential Scopes on M1 and M5 APIs (for each HTTP method). * Add OAuth Authorization Code flow and scopes to M5 APIs. | | | | | | | | |

# Notes

## Chicago

|  |  |  |  |
| --- | --- | --- | --- |
| [S4-231753](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/TSGS4_126_Chicago/Docs/S4-231753.zip) | [5GMS\_Pro\_Ph2]: Extending 5GMS with Oauth 2.0 support | Ericsson LM | Thorsten Lohmar |

**Email Discussion:**

**Presenter**: Thorsten Lohmar

**Online Discussion**:

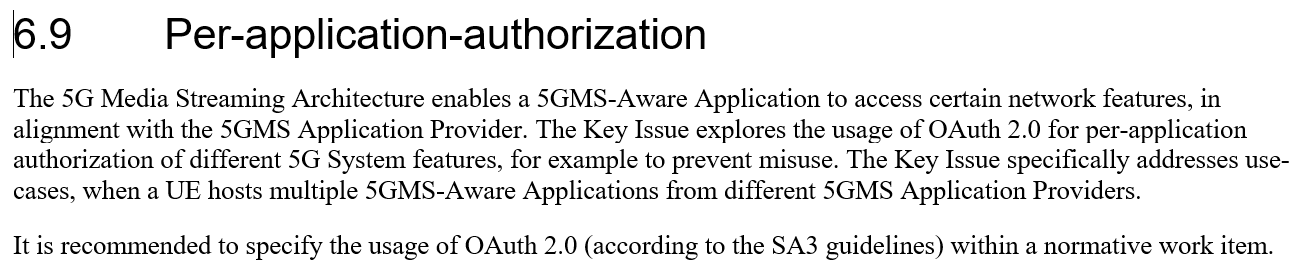
* Richard: Is the idea to obtain an authorization code, and use it subsequently in M5
* Thorsten: Yes
* Richard: Do we need this kind of security (oauth) at M5? Understand for M1. We got a security network right. What are you protecting against
* Thorsten: For example, you could have applications using policy templates of other applications that it is not intended to use
* Imed: Just to follow up, this is calls invoked my MSH, not by application. Maybe we need to dig deeper. Where will the MSH get it
* Thorsten: In 26804, we have done some scenarios. People should start looking

**Decision**:

[S4-231753](https://www.3gpp.org/ftp/TSG_SA/WG4_CODEC/TSGS4_126_Chicago/Docs/S4-231753.zip) is **endorsed**.

## Background

TR 26.804, Clause 6.9



## Summary of the Proposal in the CR

* For M1 APIs, Oauth 2.0 Client Credential flows is added to the yaml definition. CT supports Client Credentials for its NEF APIs.
* For M5 APIs, Oauth 2.0 Client Credential and Authorization Code flows are added. Support for Authorization Code is an outcome of the Study in TR 26.804.
  + Currently, CC and AC is added only to the C.4.1 M5\_ServiceAccessInformation API. Once the principle is agreed, the same definition should be added to all M5 APIs.

## Open Questions, for discussion

* OAuth Client Credential flow is a so-called 2-legged authorization flow, which does not involve a user or a resource owner. OAuth Authorization Code flow is a so-called 3-legged authorization flow. It is for discussion, whether the OAuth Client Credentials flow is suitable for M5, or whether only the Authorization Code Flow should be supported.
* TS 29.122 / 29.522 does not include any scopes within the security schemes. 5GMS M1 APIs support different features, like content hosting configuration, content preparationm, etc procedures. It is for discussion, whether the SA4 yaml definition should define different scopes, allowing control of different features and also allowing control of the operations (like read-only vs write and delete)

# Detailed Background

### Summary of Clause 5.9.2 and 5.9.3 of TR 26.804

### 5.9.2 Collaboration Scenarios

Collaboration A: UE hosting multiple Applications (Multiple Applications on the same UE)

Collaboration B: Applications with multiple subscription levels (Same Application, but with different levels)

### 5.9.3 Role distribution in the 5GMS deployments

The 5G Media Streaming architecture can be used for different application service offerings. Annex A in TS 26.512 [16] describes three different Dynamic Policy usage examples: Premium QoS, Conditional Zero Rating and Background Download. In all the three cases, different network features are used to realise the Dynamic Policy, e.g. an increase in network resource utilization when consuming HD content with the corresponding network QoS.

It is assumed in all three examples that the 5GMS Application Provider (and the Application Service Provider) has an agreement with the 5G System provider to use the relevant network feature.

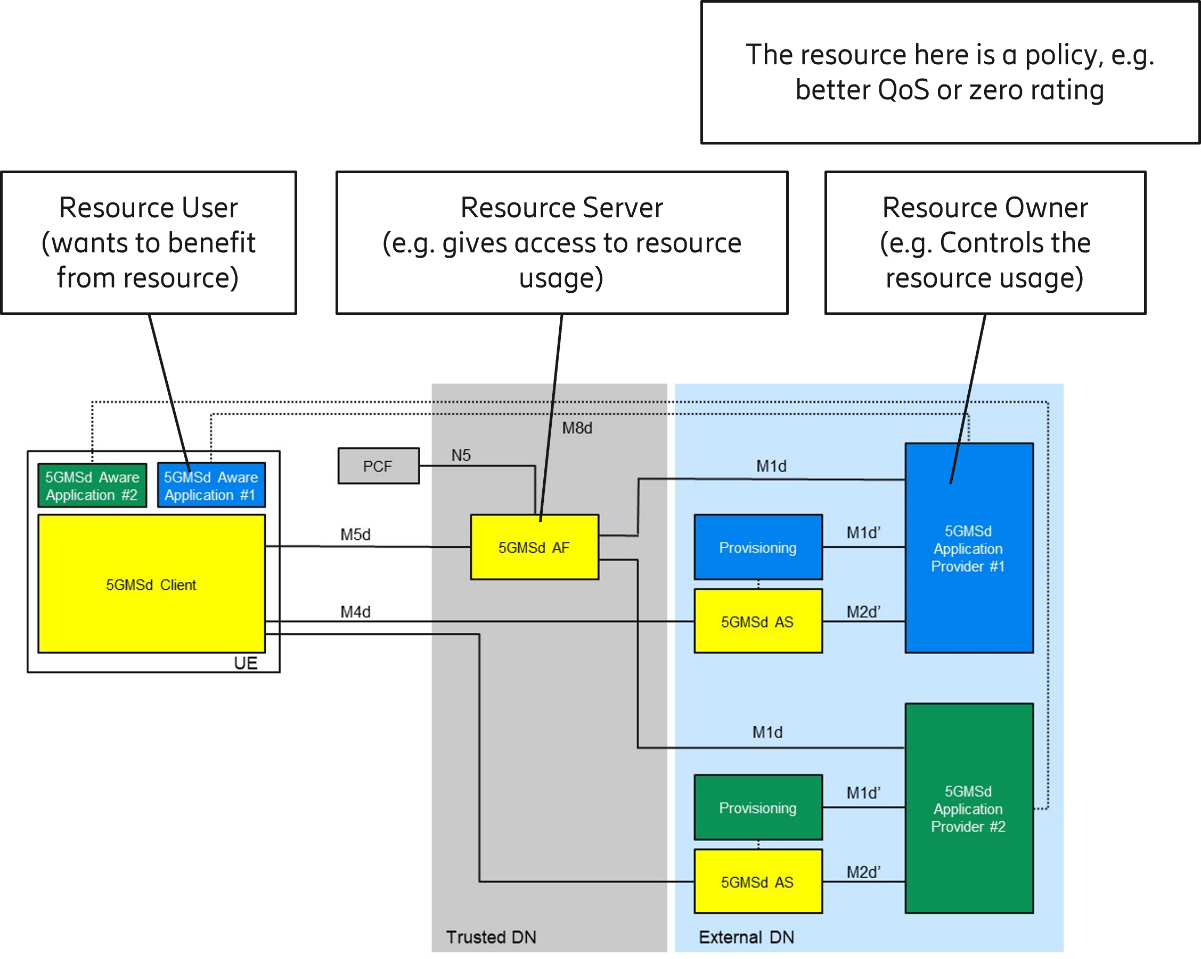


Figure 5.9.3-1: Applying roles for 5G Media Streaming Architecture functions

Figure 5.9.2-1 illustrates the different roles and responsibilities:

- The resource in question is a network policy.

- The 5G System Provider is the resource owner in this case, since it provides the 5G connectivity service.

- The 5GMSd-Aware Application is the Resource User. It instructs the 5GMSd Client to activate a certain dynamic policy, based on the service subscription and the selected content.

- The 5GMS Application Provider is the Resource Owner. It checks that the requested dynamic policy matches the application service subscription. For example (with reference to clause A.2 in TS 26.512 [16]), when the user has an HD video subscription, the user should only be authorised to activate a dynamic policy corresponding to the HD operating point.

\*\*\*\* First Change for TS 26.510 \*\*\*\*

## 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

…

[RFC5246] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[RFC8446] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[RFC6749] IETF RFC 6749: "The OAuth 2.0 Authorization Framework", October 2012.

[29222] 3GPP TS 29.222: "Common API Framework for 3GPP Northbound APIs; Stage 3".

\*\*\*\* Next Change \*\*\*\*

## 7.4 Security

### 7.4.1 General

The Media AF shall enable secure provision of information in the Media Delivery System by authenticated and authorised Media-aware Applications or Media Application Providers.

### 7.4.2 Authorising Media Application Provider access to the Media AF at reference point M1

When a Media Application Provider deployed outside the Trusted DN attempts to access a Media AF deployed inside the Trusted DN, the Media Delivery System shall authenticate and authorise the Media Application Provider.

Access to the Maf\_Provisioning API of the Media AF by the Media Application Provider at reference point M1 may be authorised by means of the OAuth 2.0 protocol specified in RFC 6749 [RFC6749]), using the *client credentials* authorization grant.

When CAPIF (see TS 29.222 [29222]) is used for external API exposure:

- The CAPIF core function shall play the role of authorization server, the Media AF shall play the role of resource server and the Media Application Provider shall play the role of client.

- Before invoking any service operation exposed by the Media AF, the Media Application Provider shall negotiate the security method (PKI, TLS-PSK or OAuth 2.0) with the CAPIF core function and shall ensure that the Media AF has the required credentials to authenticate access tokens subsequently presented by the Media Application Provider (see clauses 5.6.2.2 and 6.2.2.2 of TS 29.222 [29222]).

- If PKI or TLS-PSK is the selected security method between the Media Application Provider and the Media AFthe Media AF shall, upon invocation of a Maf\_Provisioning service operation by the Media Application Provider at reference point M1, retrieve the authorisation information from the CAPIF core function as described in clause 5.6.2.4 of TS 29.222 [29222].

- If OAuth 2.0 [RFC6749] is the selected security method between the Media Application Provider and the Media AF, the Media Application Provider shall, prior to invoking Maf\_Provisioning service operations on the Media AF at reference point M1, obtain an access token from the authorization server (CAPIF core function) by invoking the Obtain\_Authorization service operation specified in clause 5.6.2.3.2 of TS 29.222 [29222].

Otherwise:

- The Media AF shall play the role of both authorization server and resource server, and the Media Application Provider shall play the role of client.

- The Media Application Provider shall obtain an access token from the authorization server (Media AF) using the client credentials authorization grant specified in section 4.4 of RFC 6749 [RFC6749] prior to invoking Maf\_Provisioning service operations on the resource server (Media AF) at reference point M1.

### 7.4.3 Authorising Media Session Handler access to the Media AF at reference point M5

When a Media Session Handler deployed in a Media Client attempts to access a Media AF deployed inside the Trusted DN, the Media Delivery System shall authenticate and authorise the Media Session Handler.

Access to the Maf\_SessionHandling API of the Media AF by the Media Session Handler at reference point M5 shall be authorised by means of the OAuth 2.0 protocol specified in RFC 6749 [RFC6749], using the "Client Credentials" or "Authorization Code" flow grant types.

Editor's Note: Awaiting further contribution.

\*\*\*\* Open API \*\*\*\*

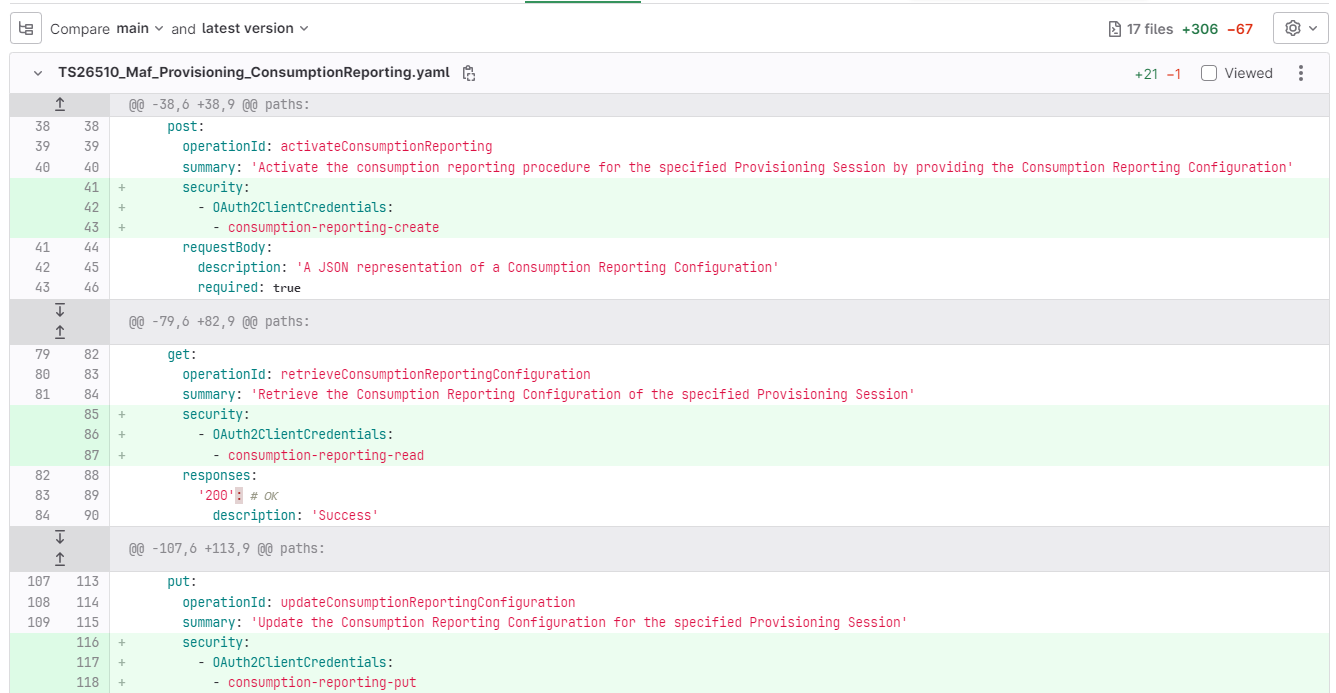
# 3GPP Forge merge request

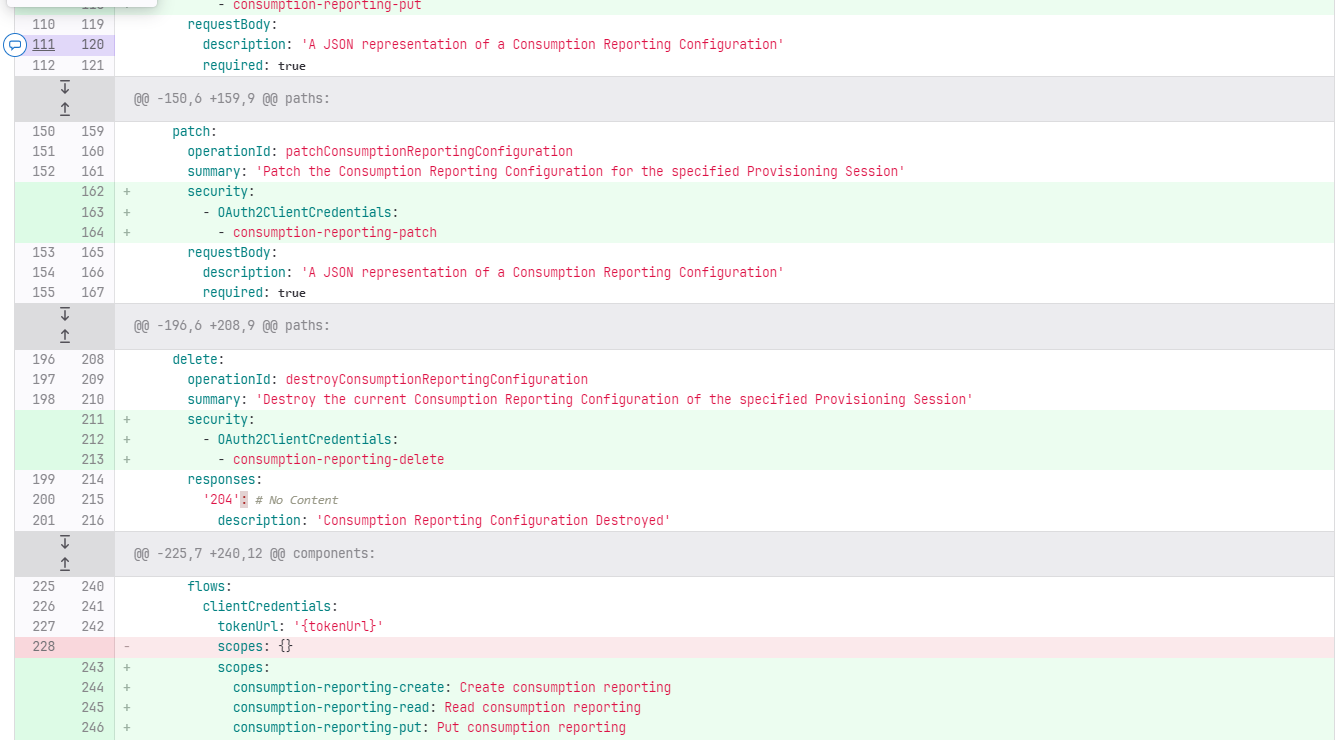
The code changes associated with this Change Request are available for review at the following URL:

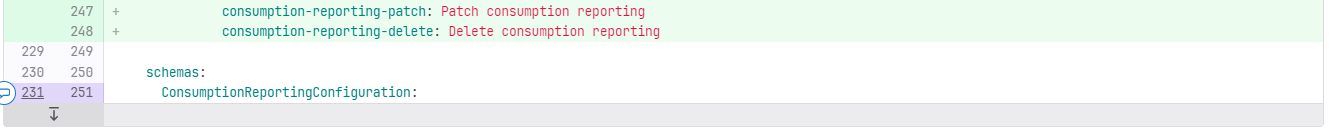
https://forge.3gpp.org/rep/sa4/5gms\_pro\_ph2/-/merge\_requests/12/diffs

The proposed changes are reproduced below for posterity:

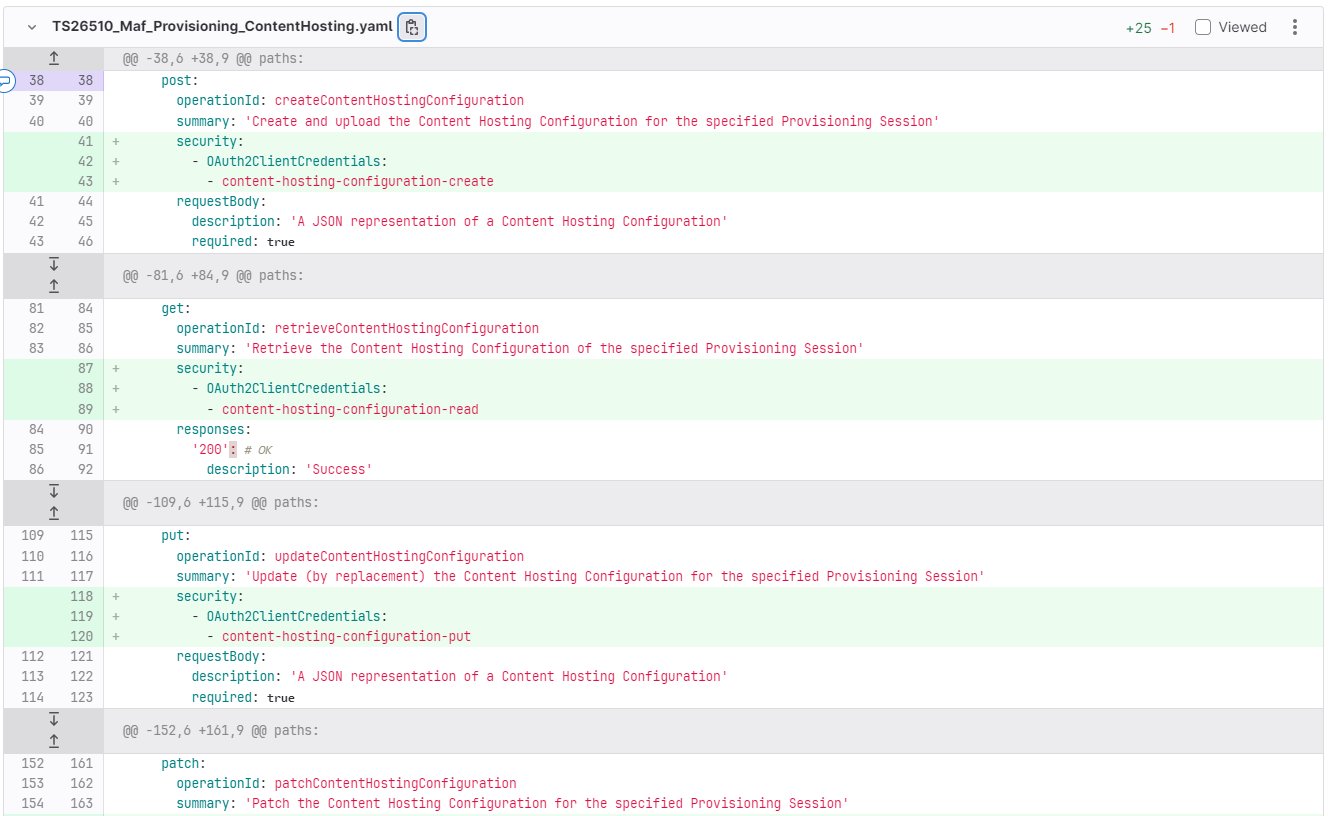
The OAuth 2.0 specific definitions follow [OAuth 2.0 (swagger.io)](https://swagger.io/docs/specification/authentication/oauth2/)

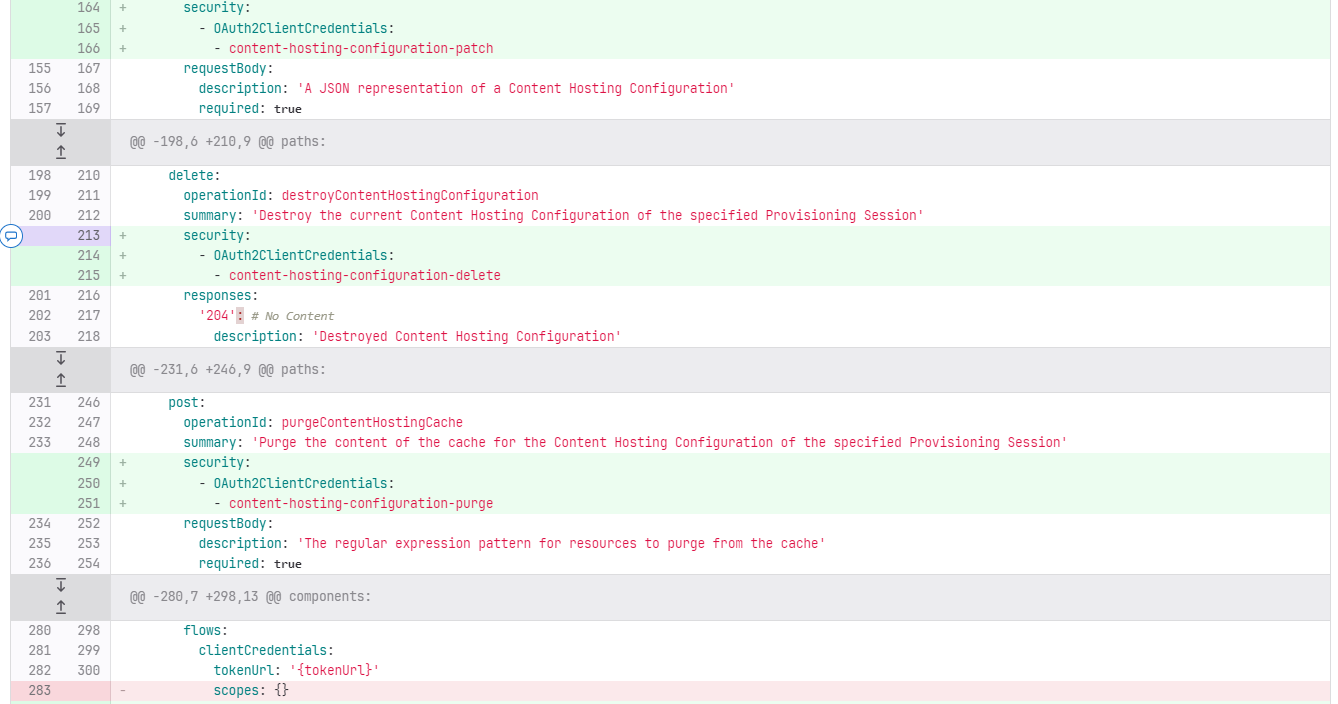


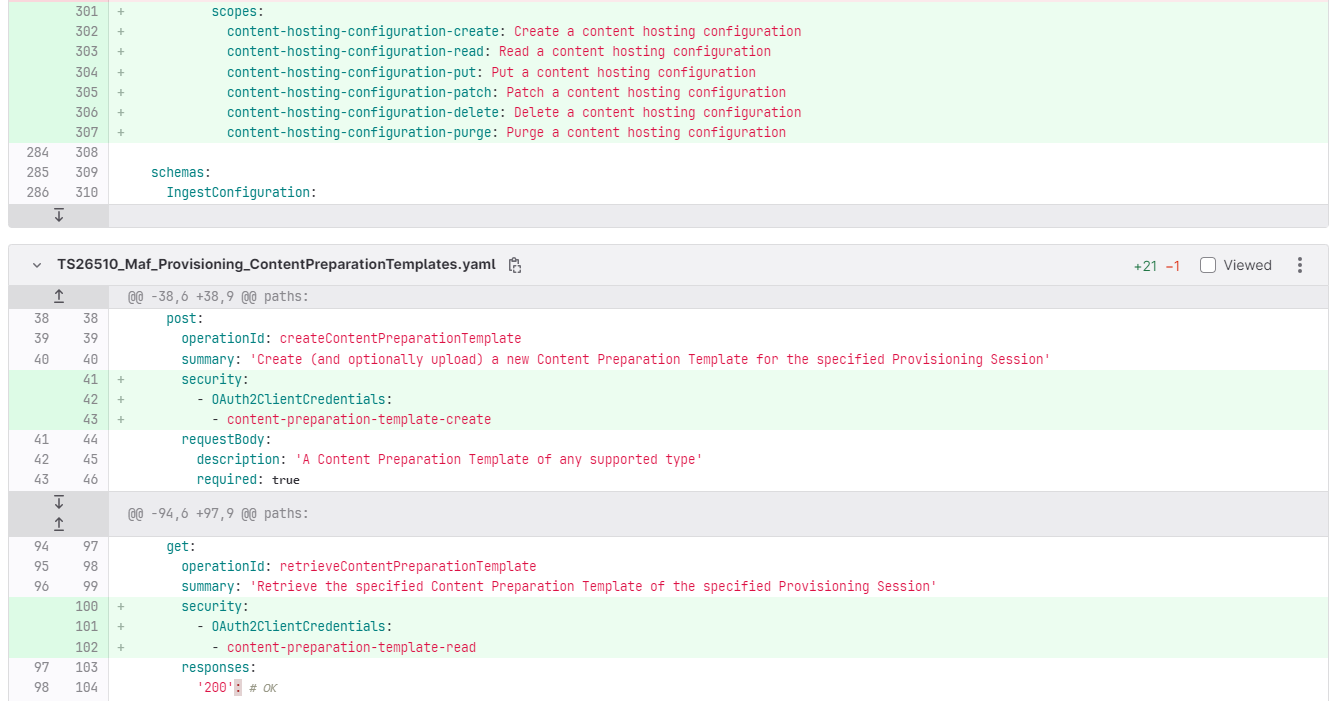


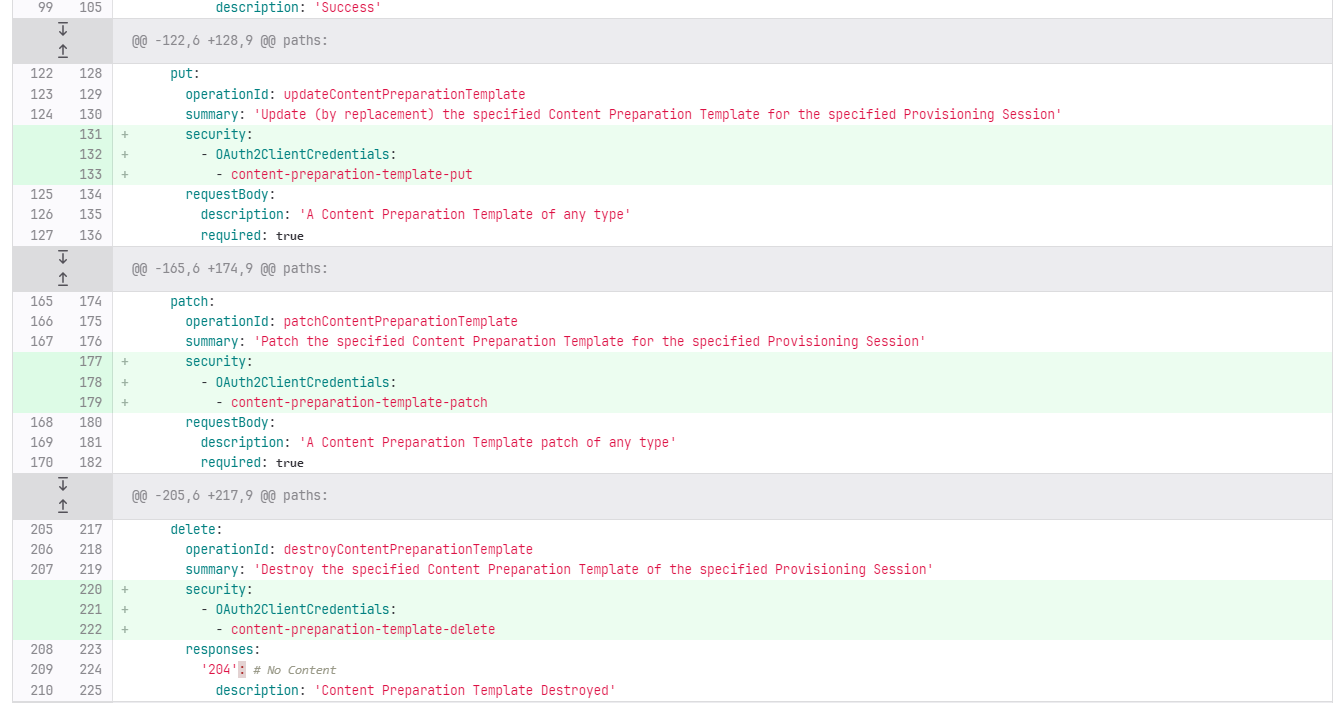


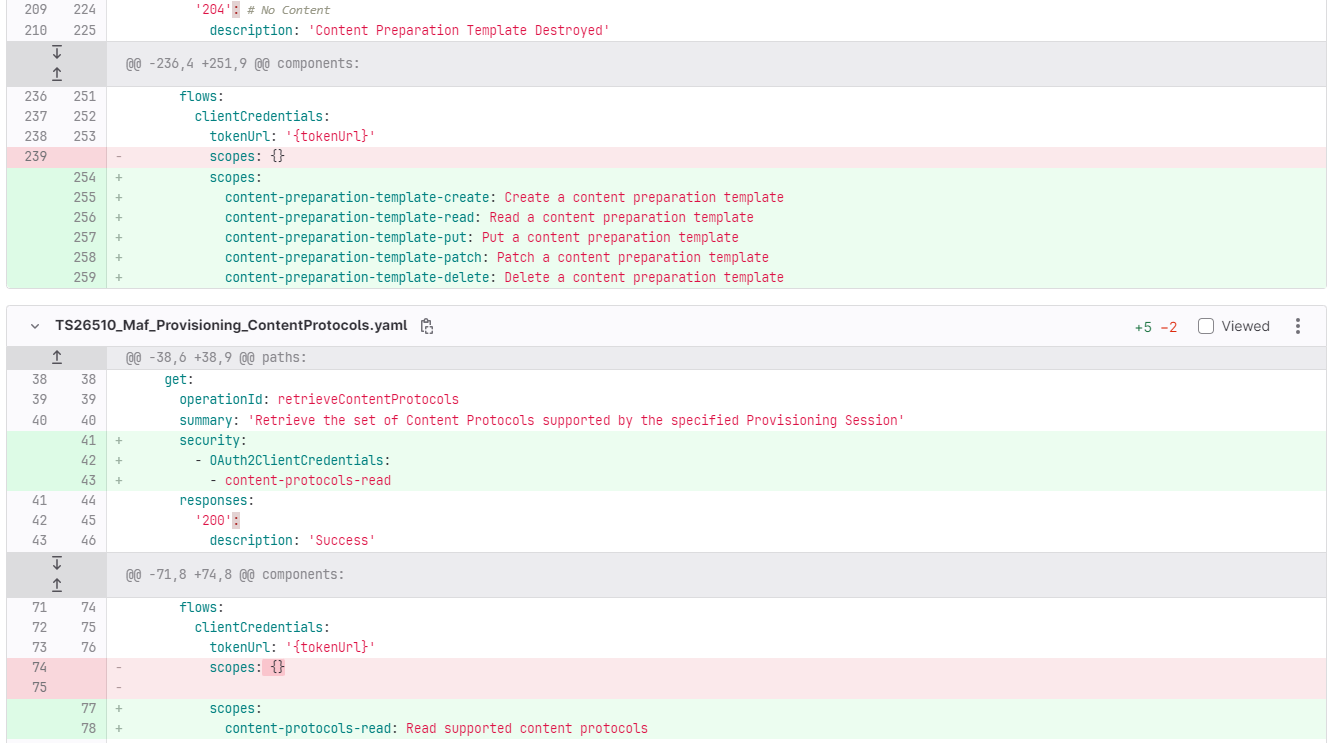
TS26510\_Maf\_Provisioning\_ContentHosting.yaml

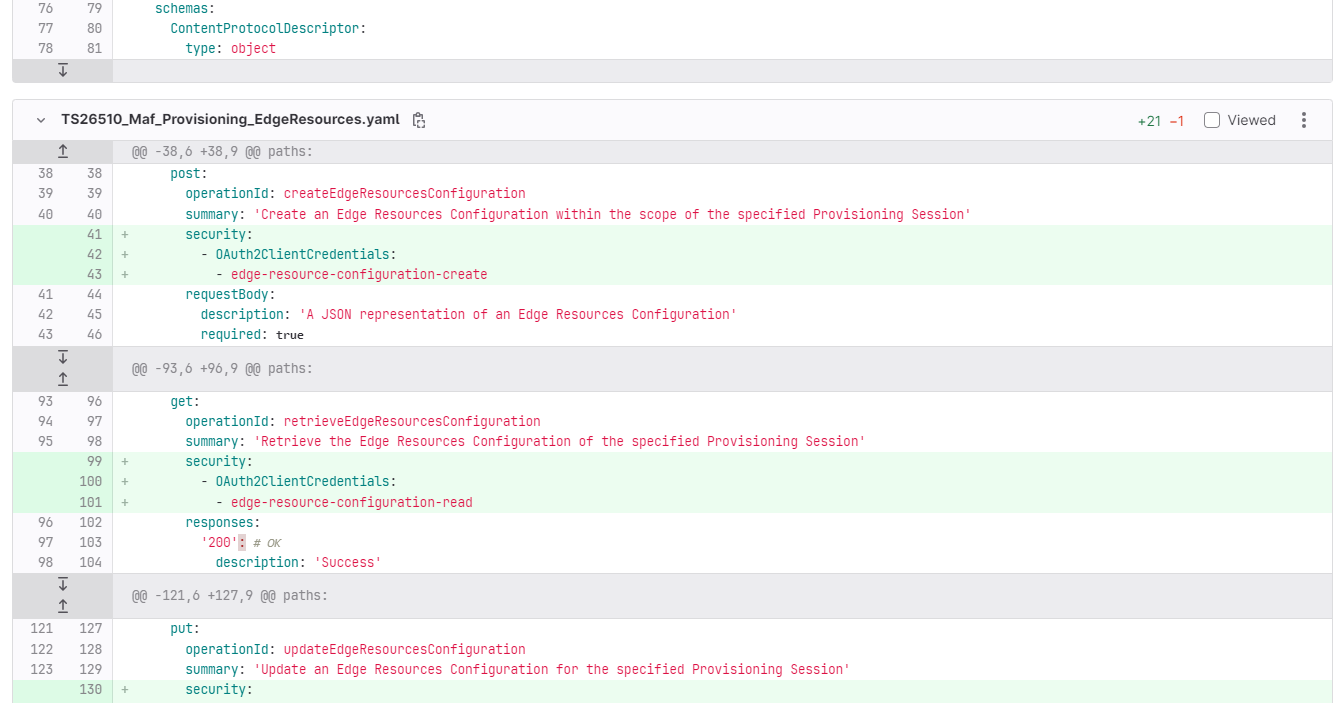


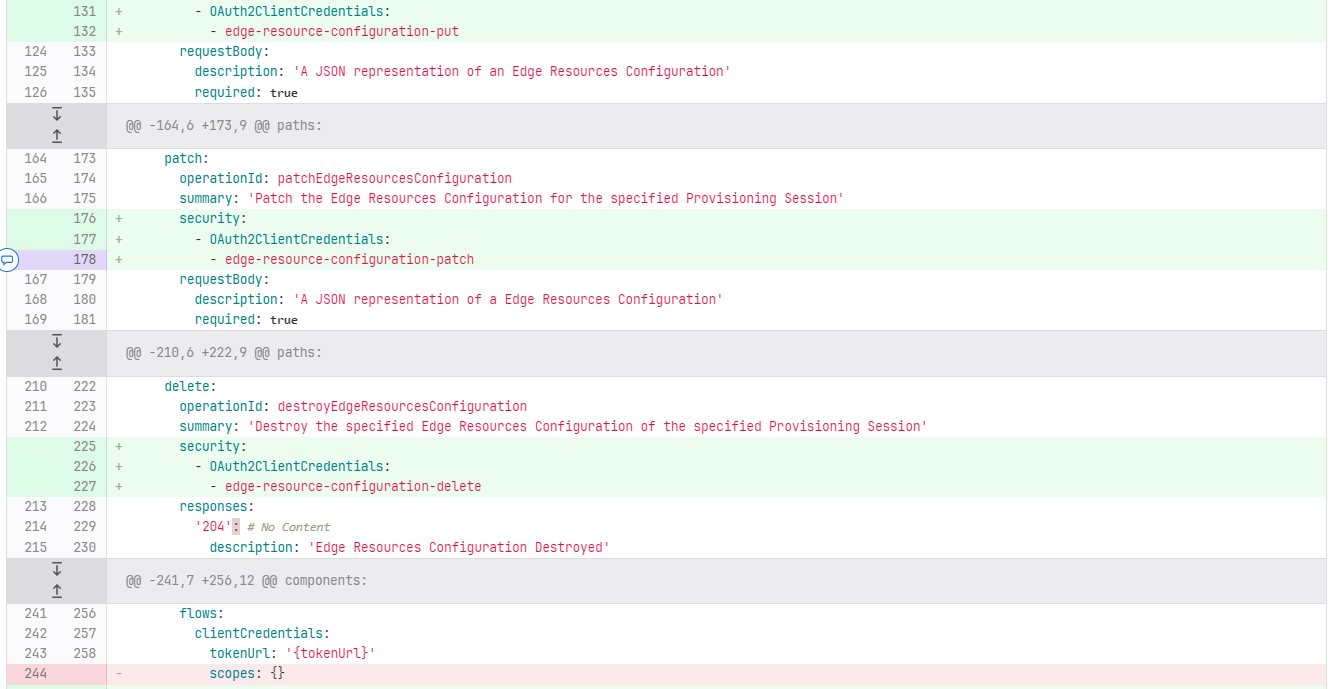


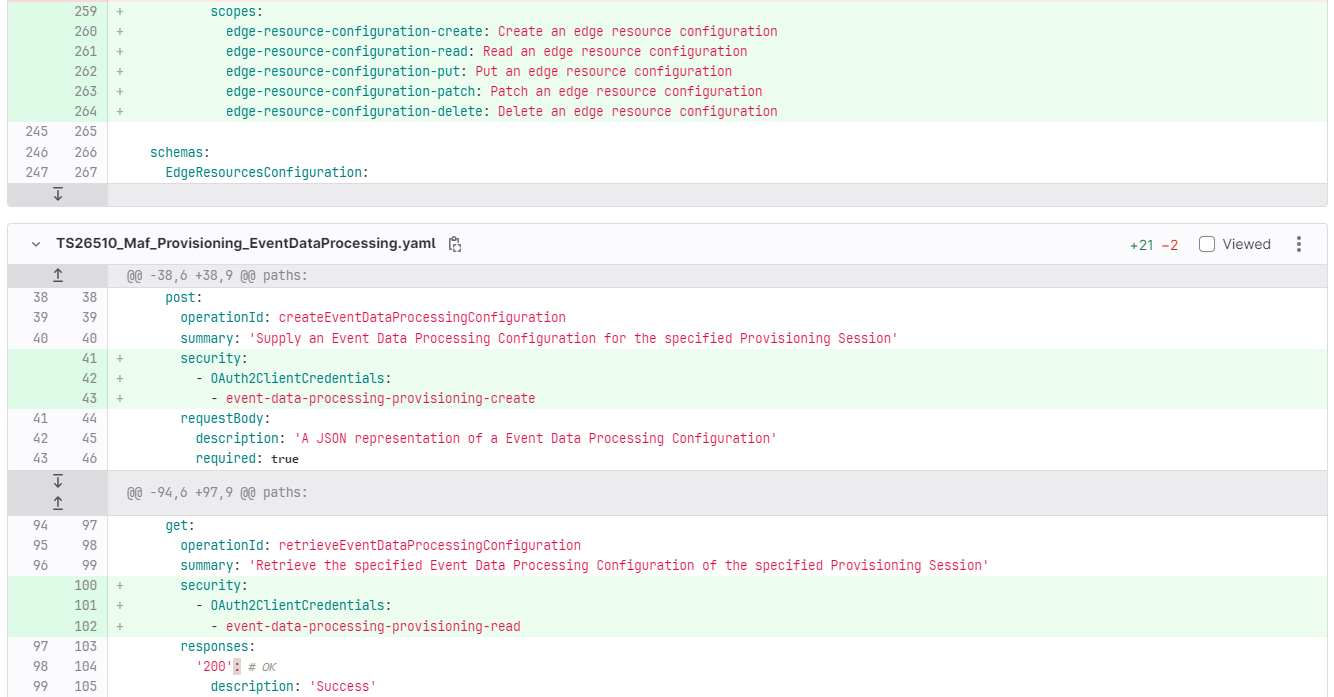




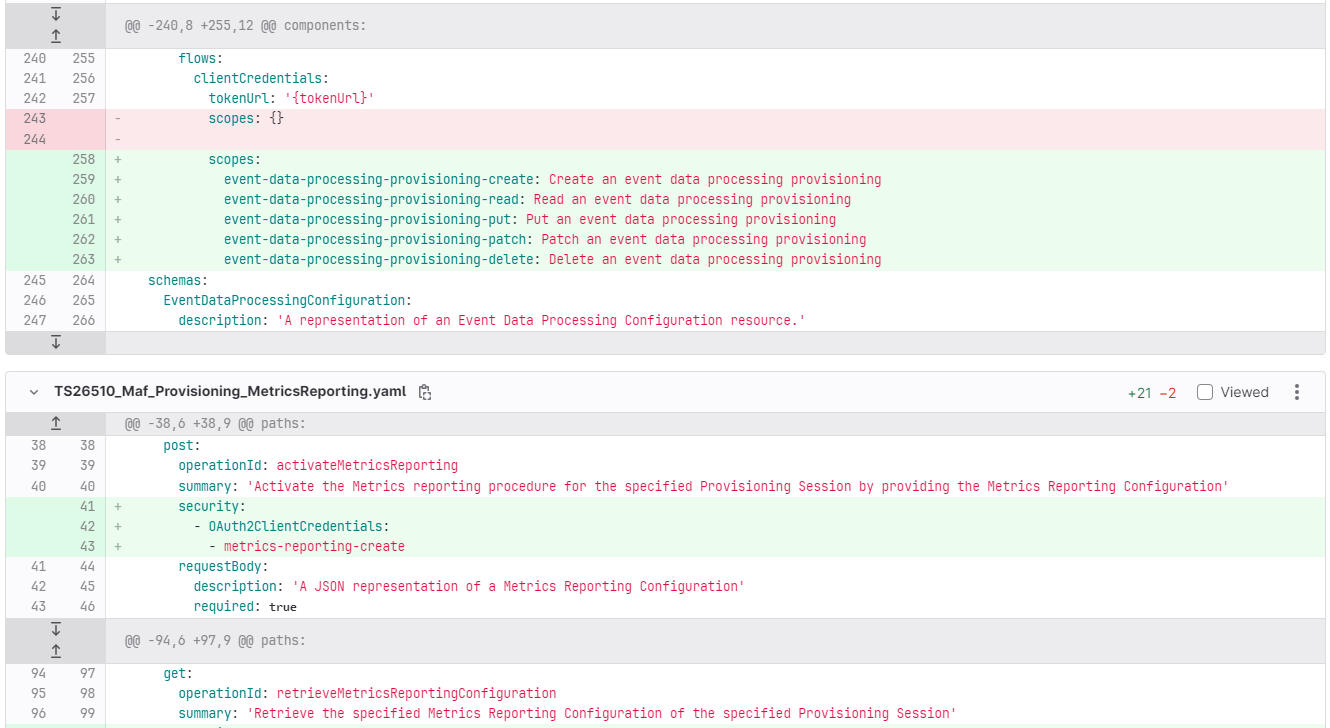


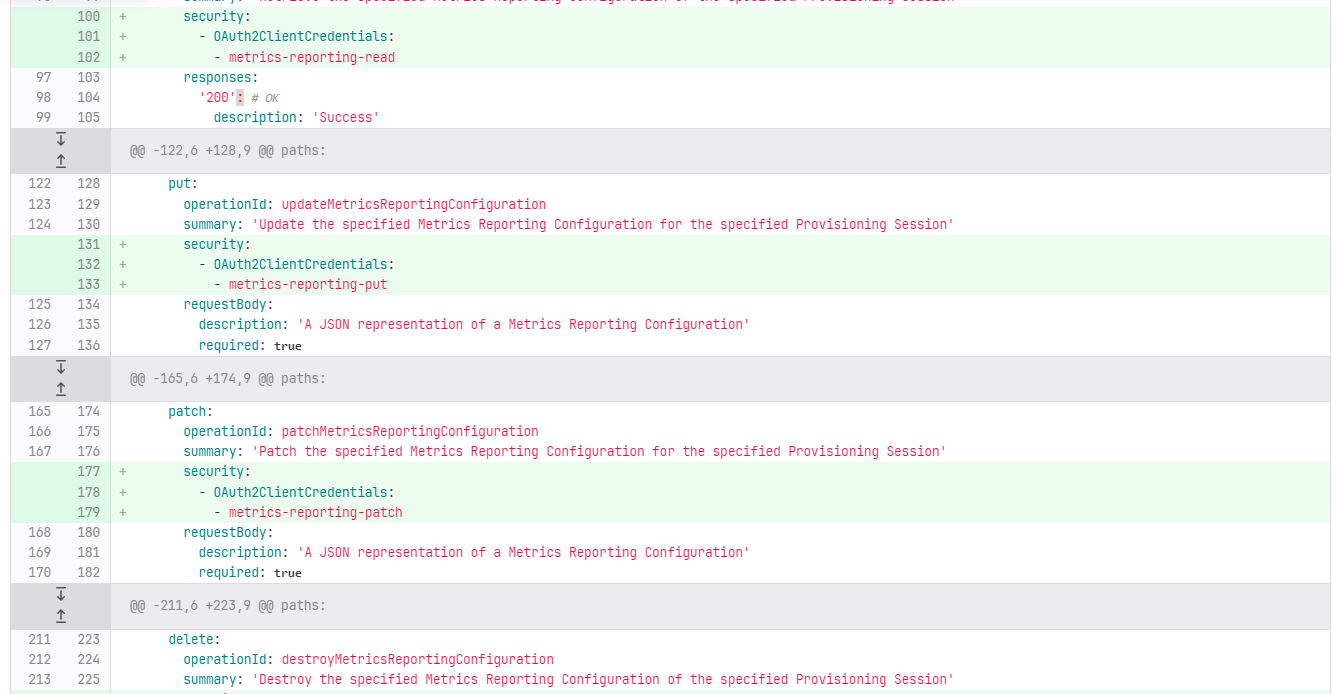


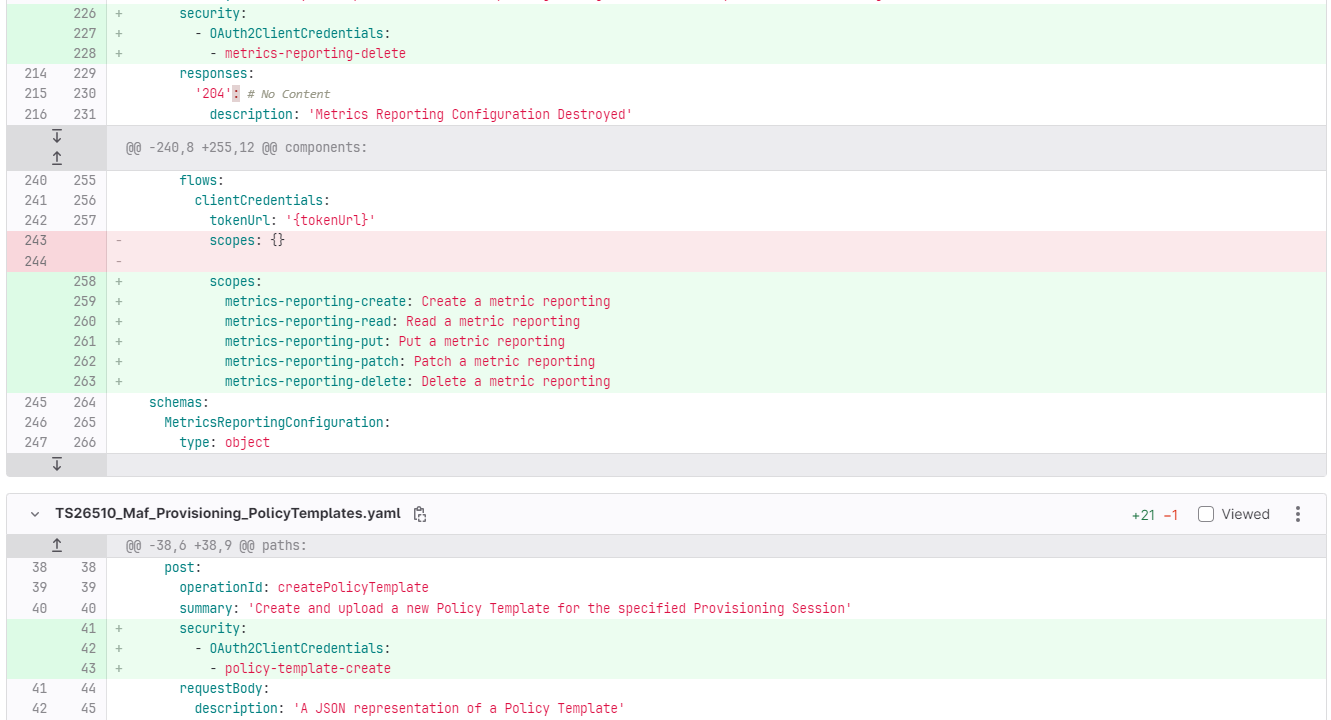


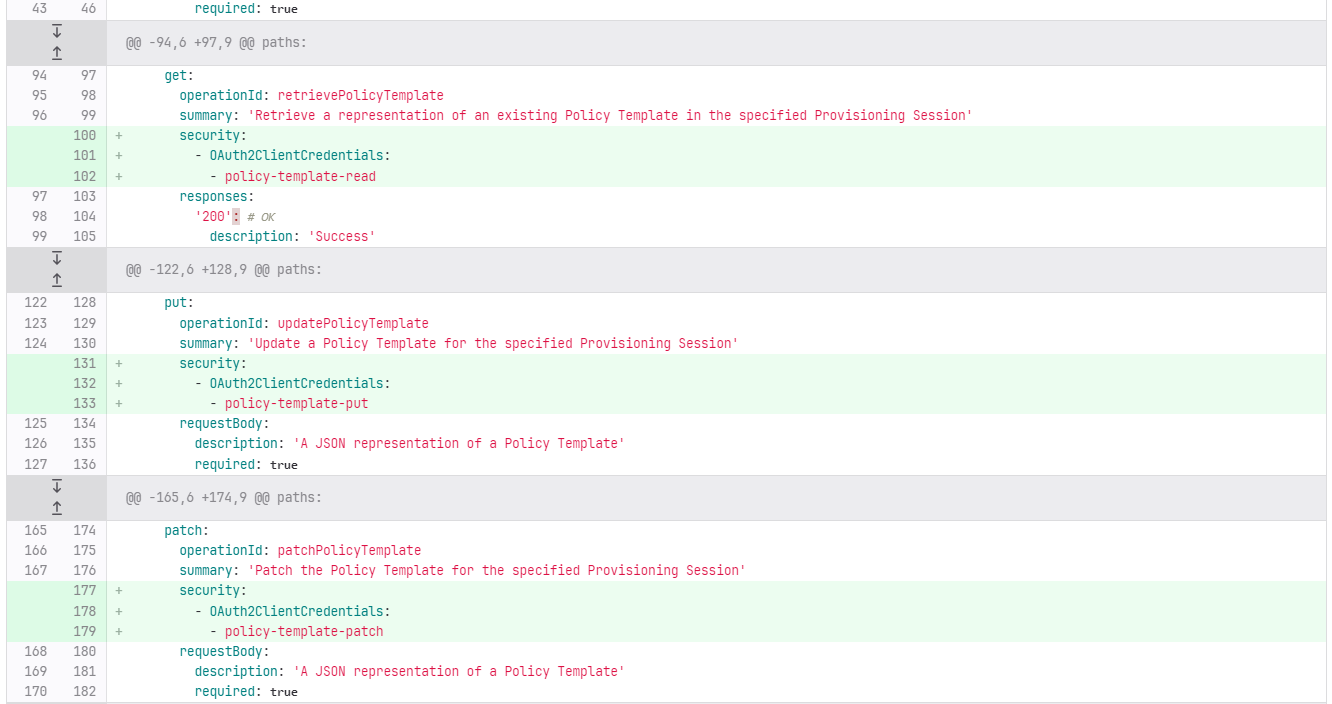


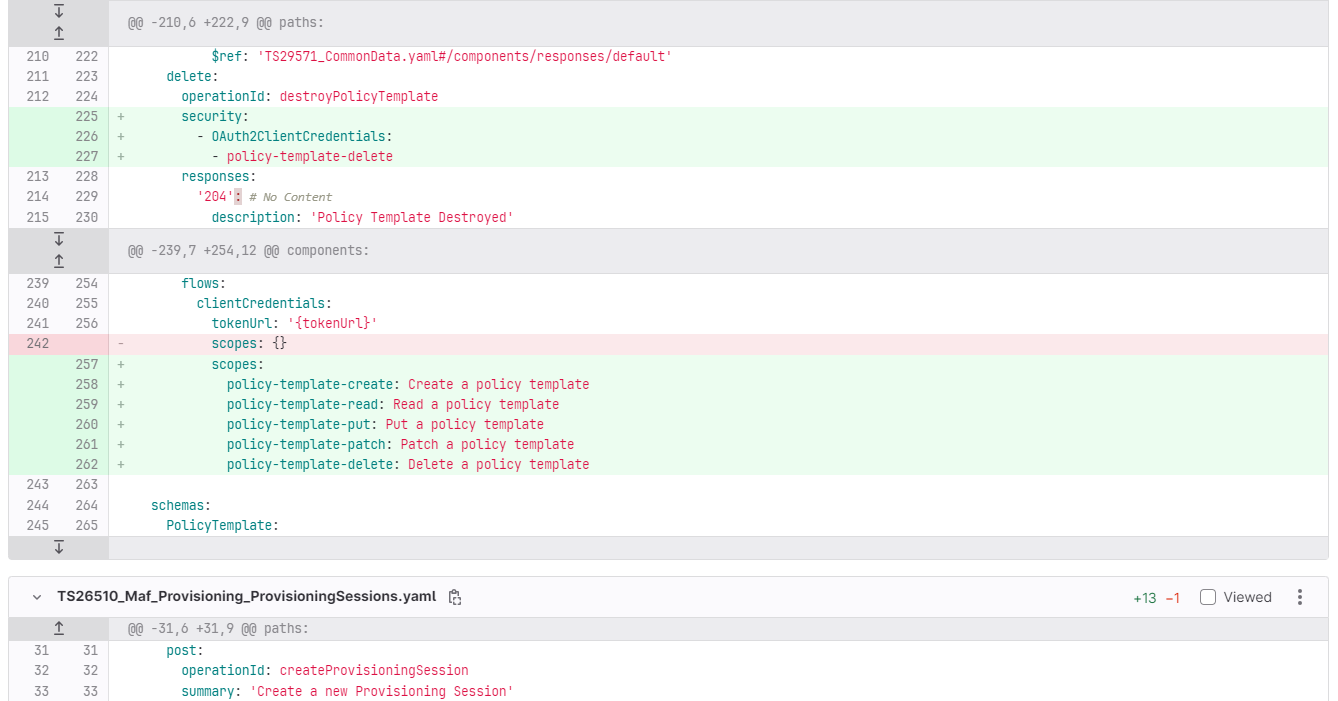


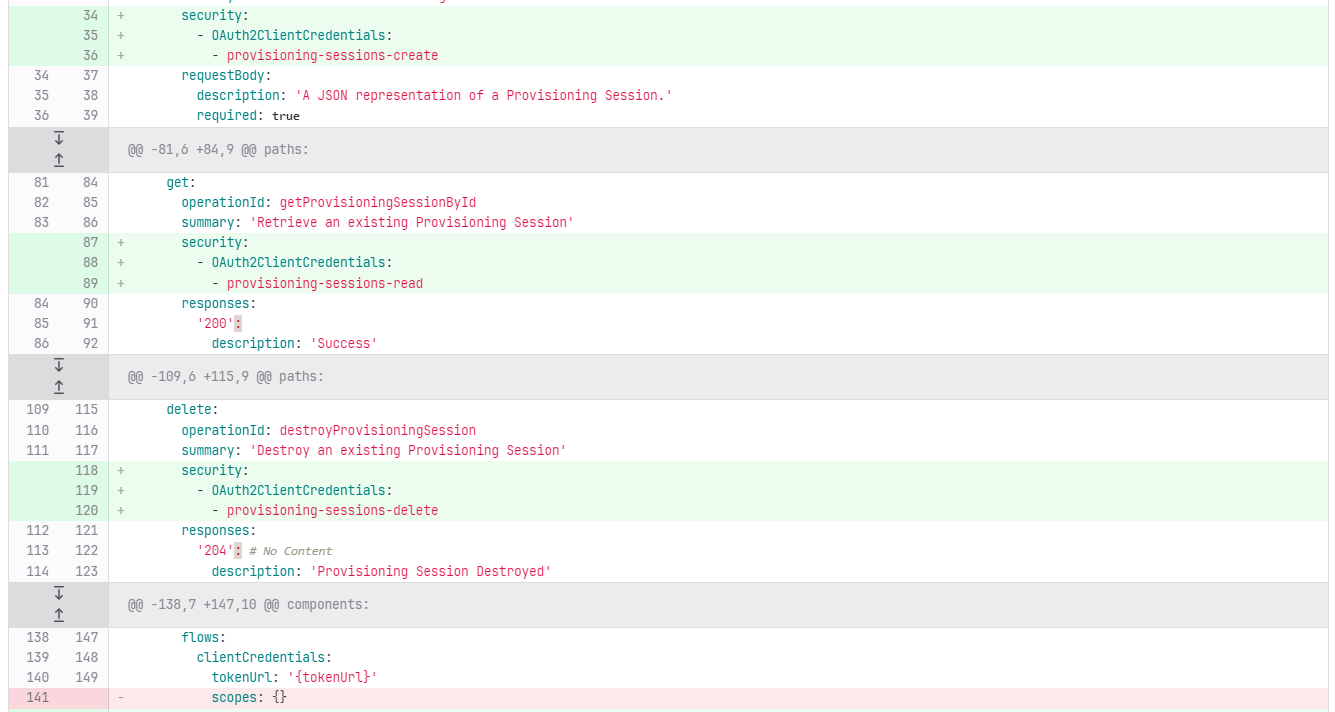




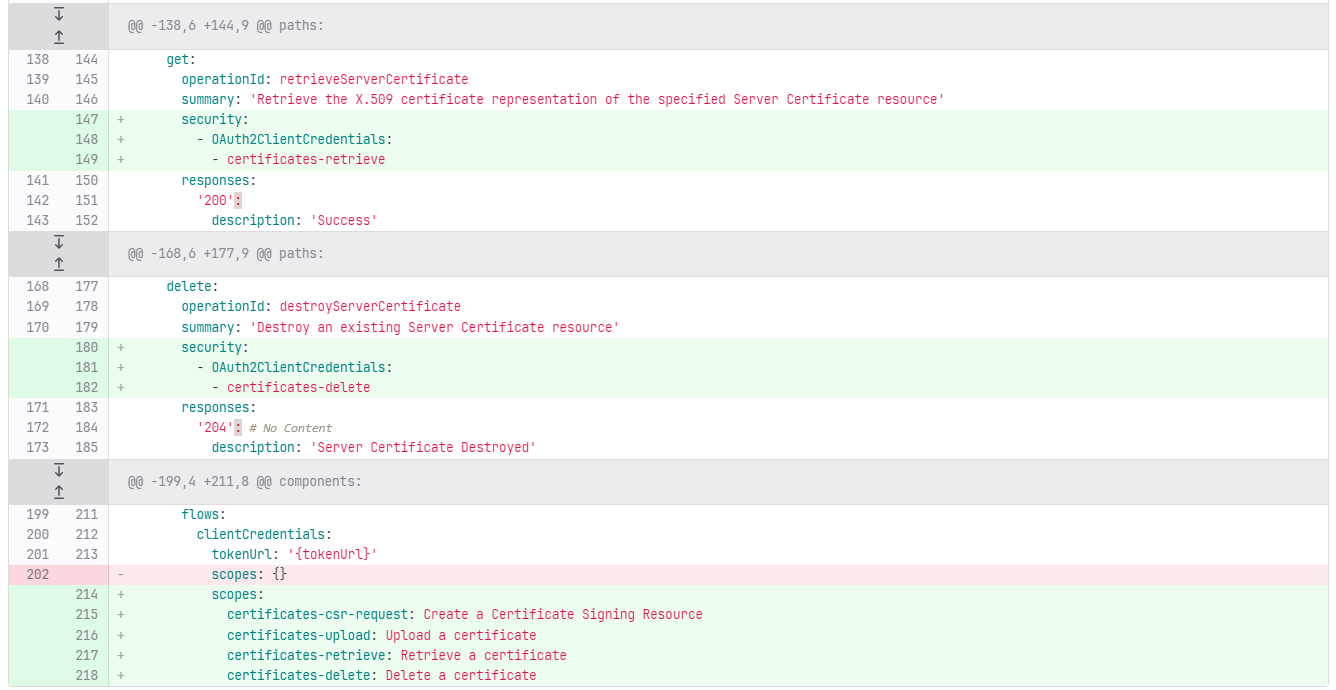


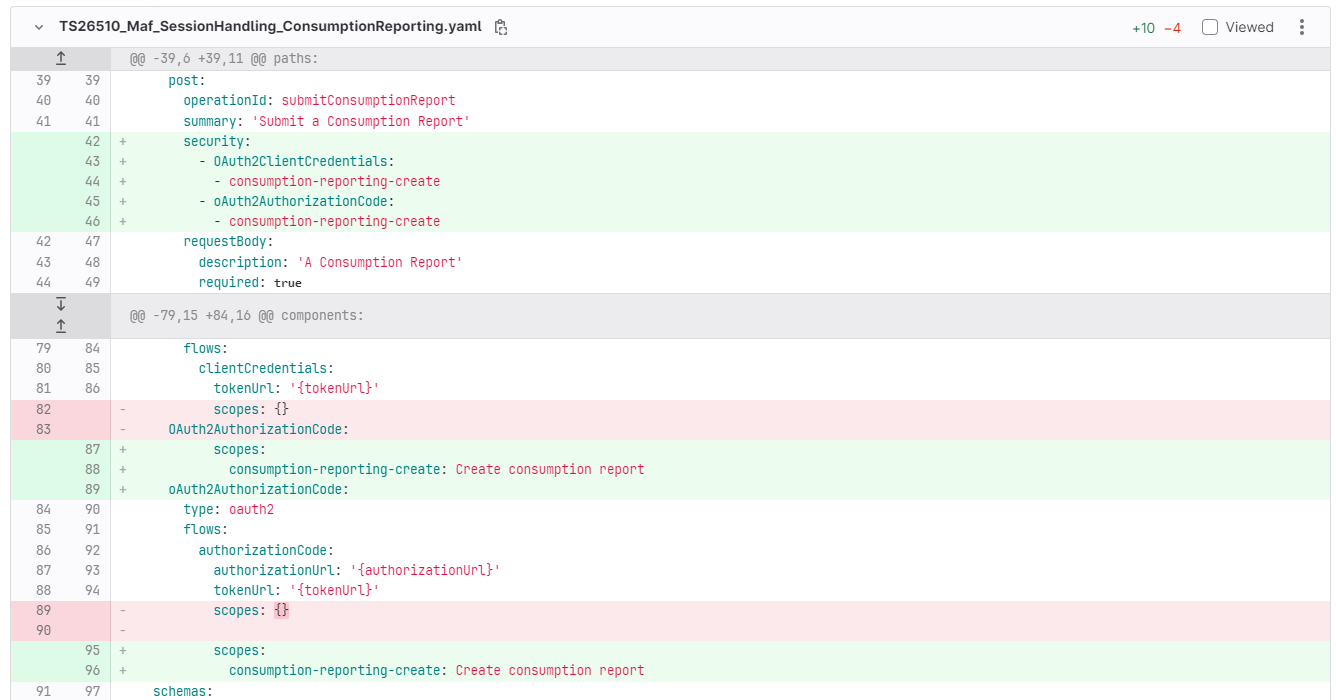


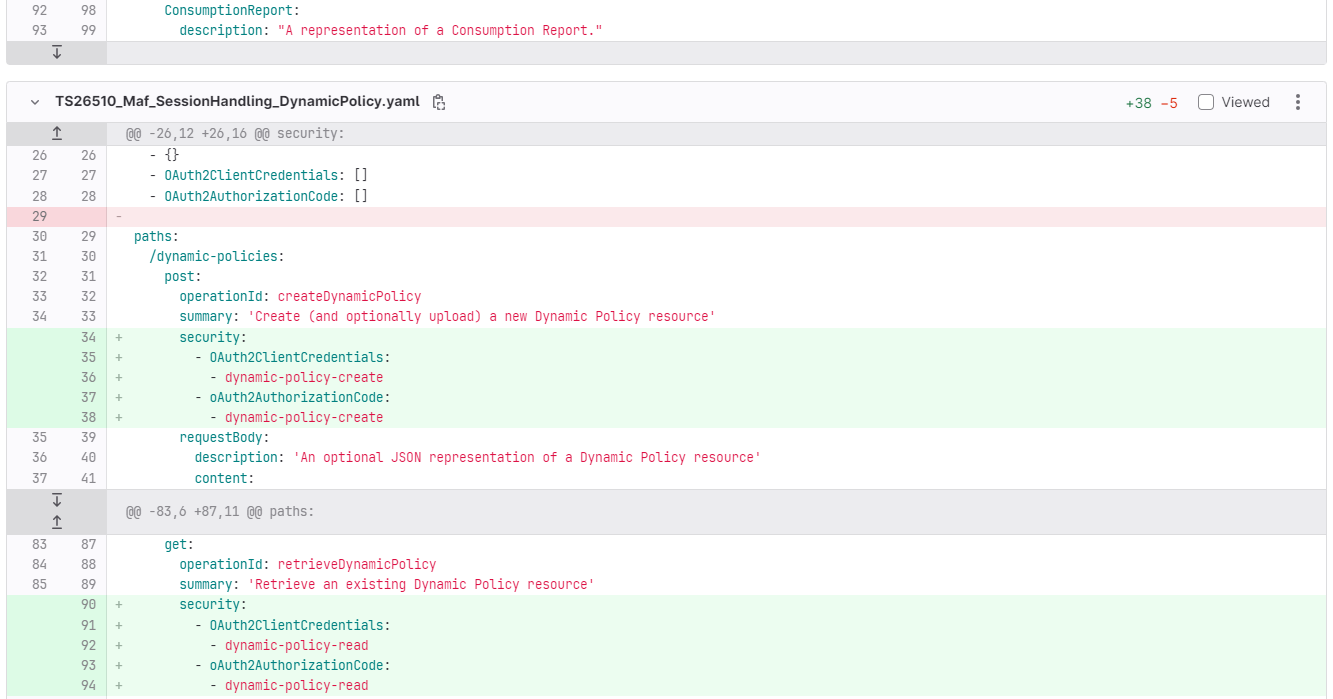


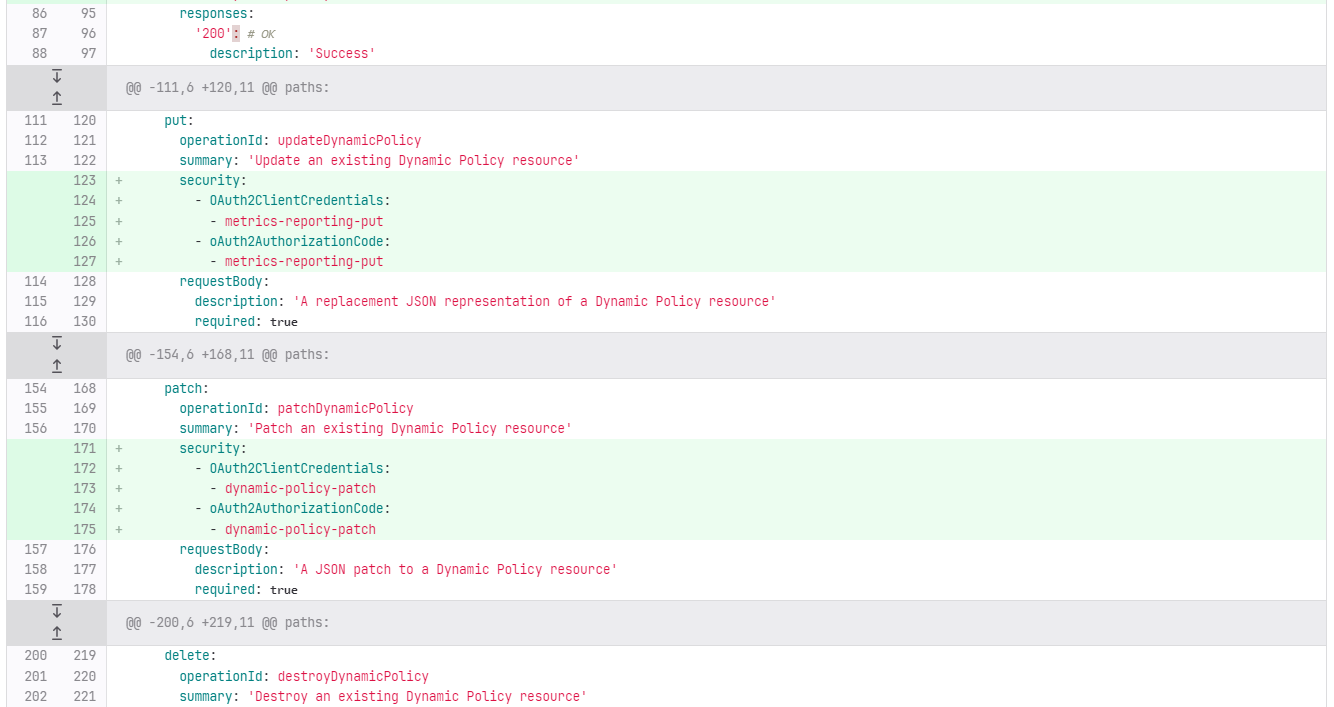


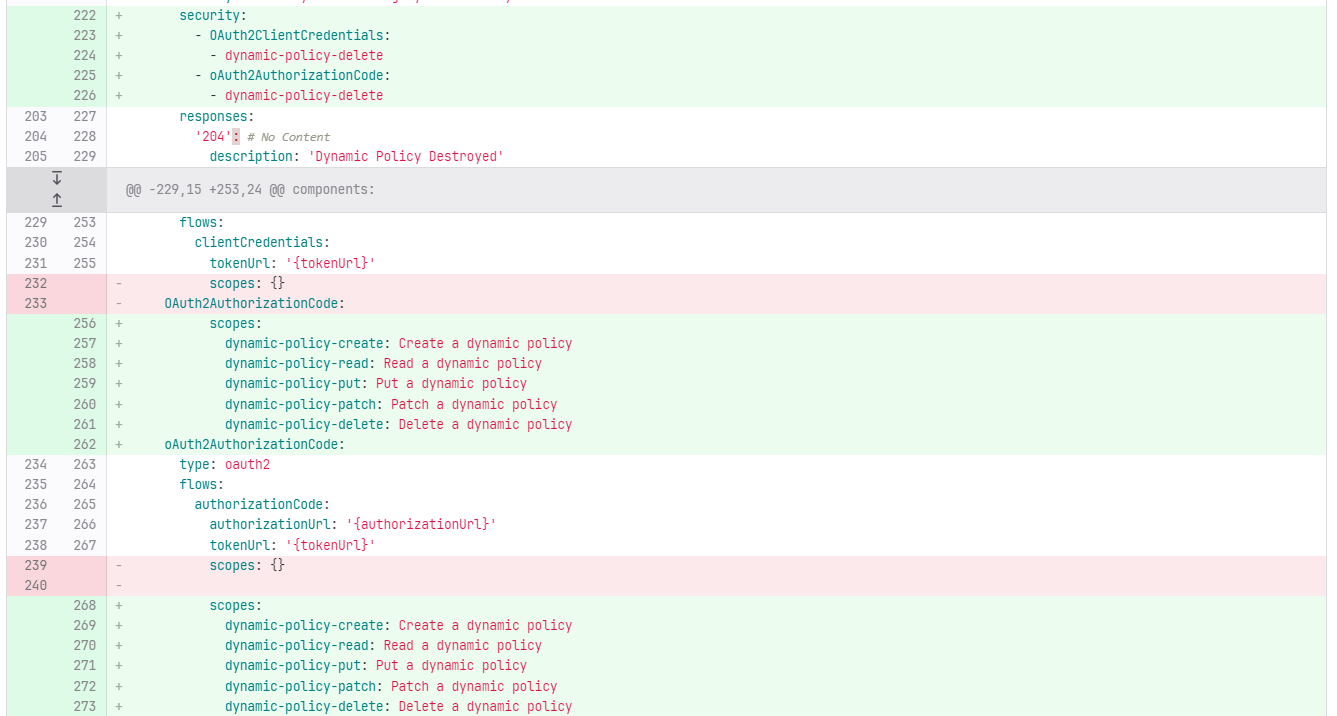


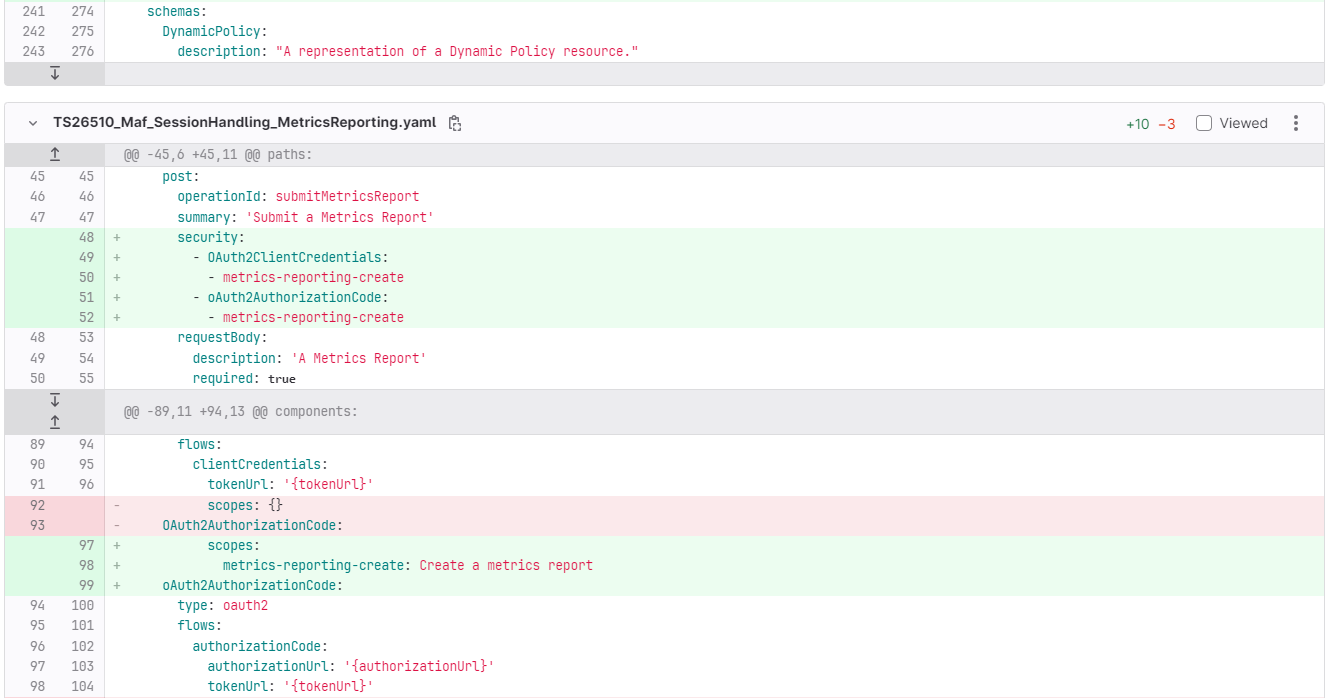


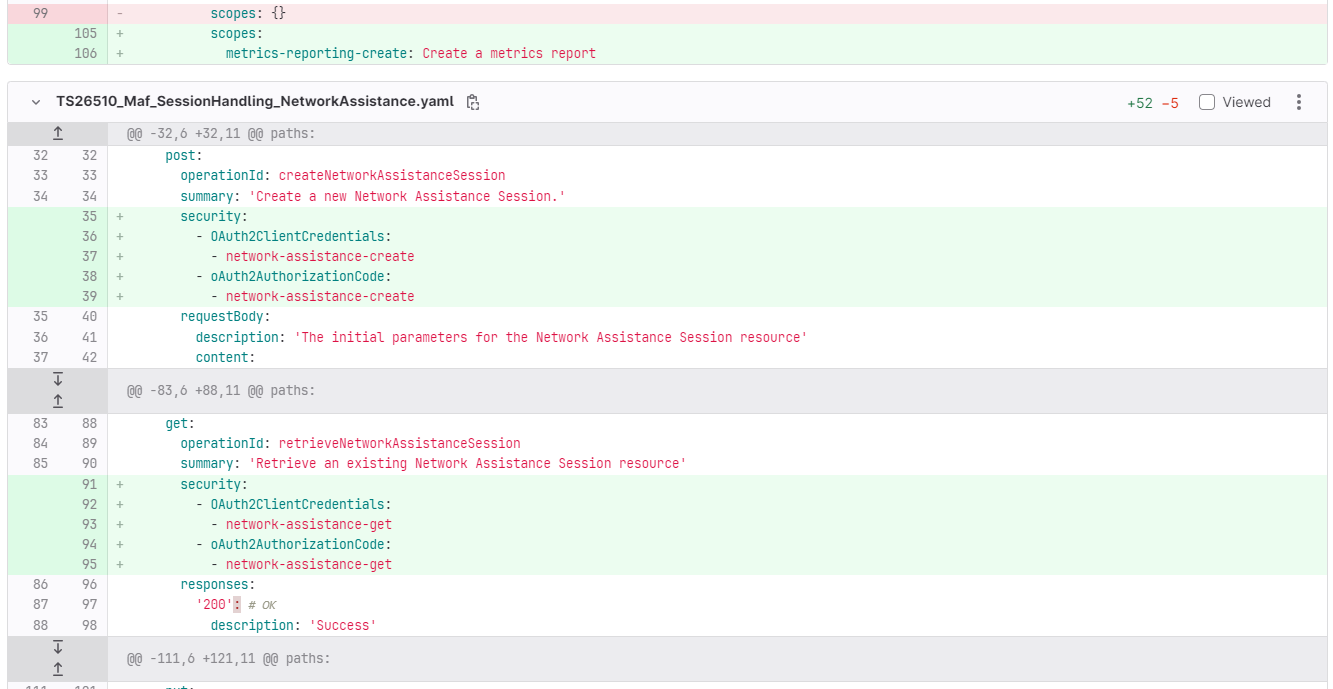


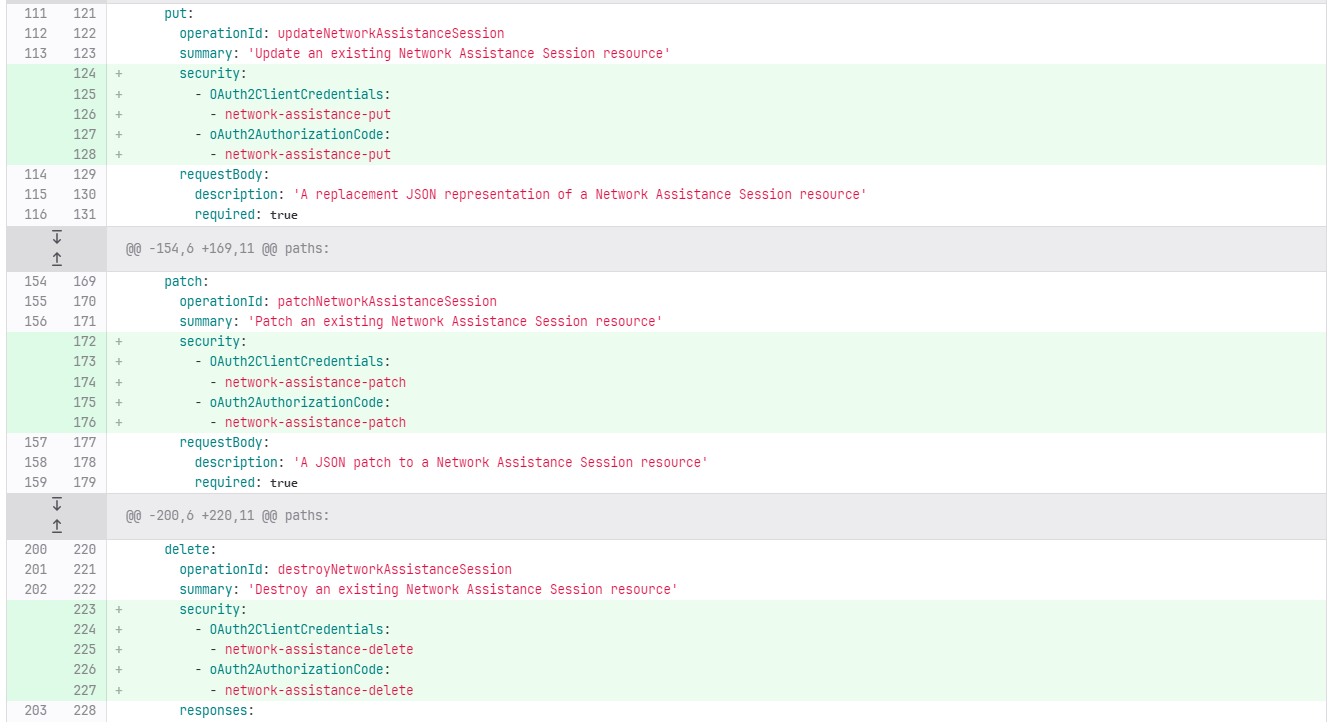


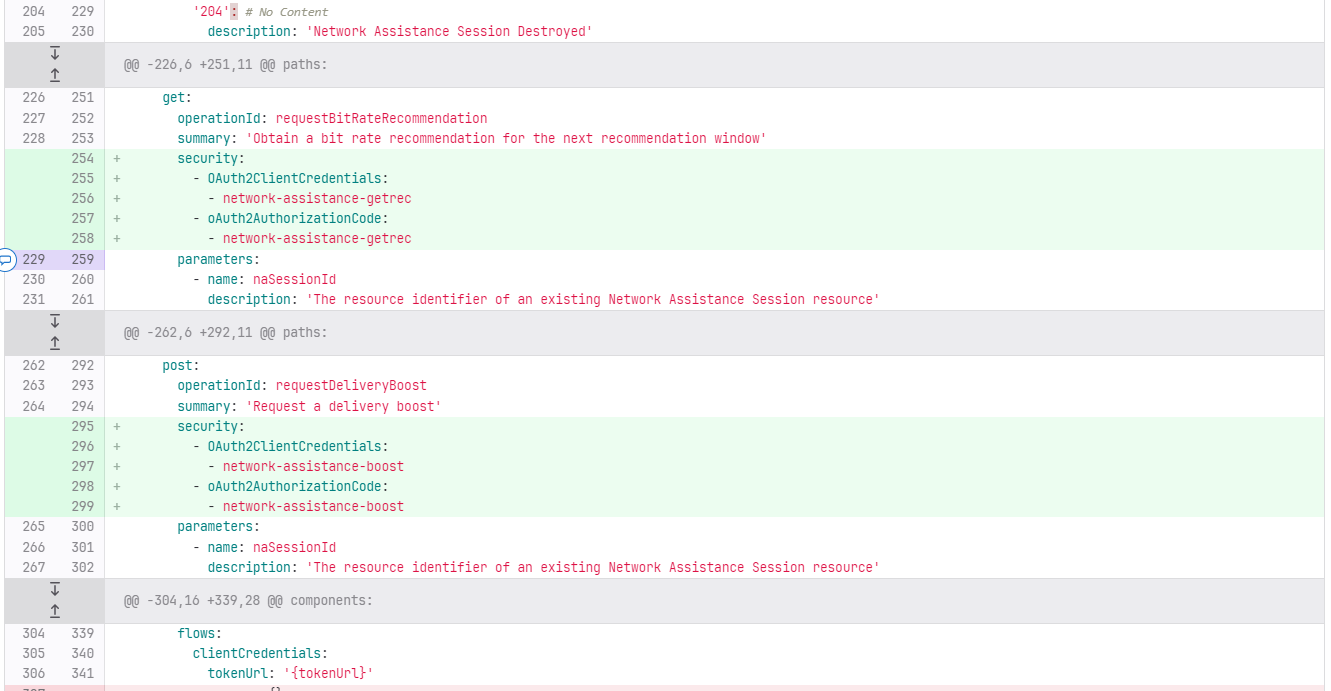


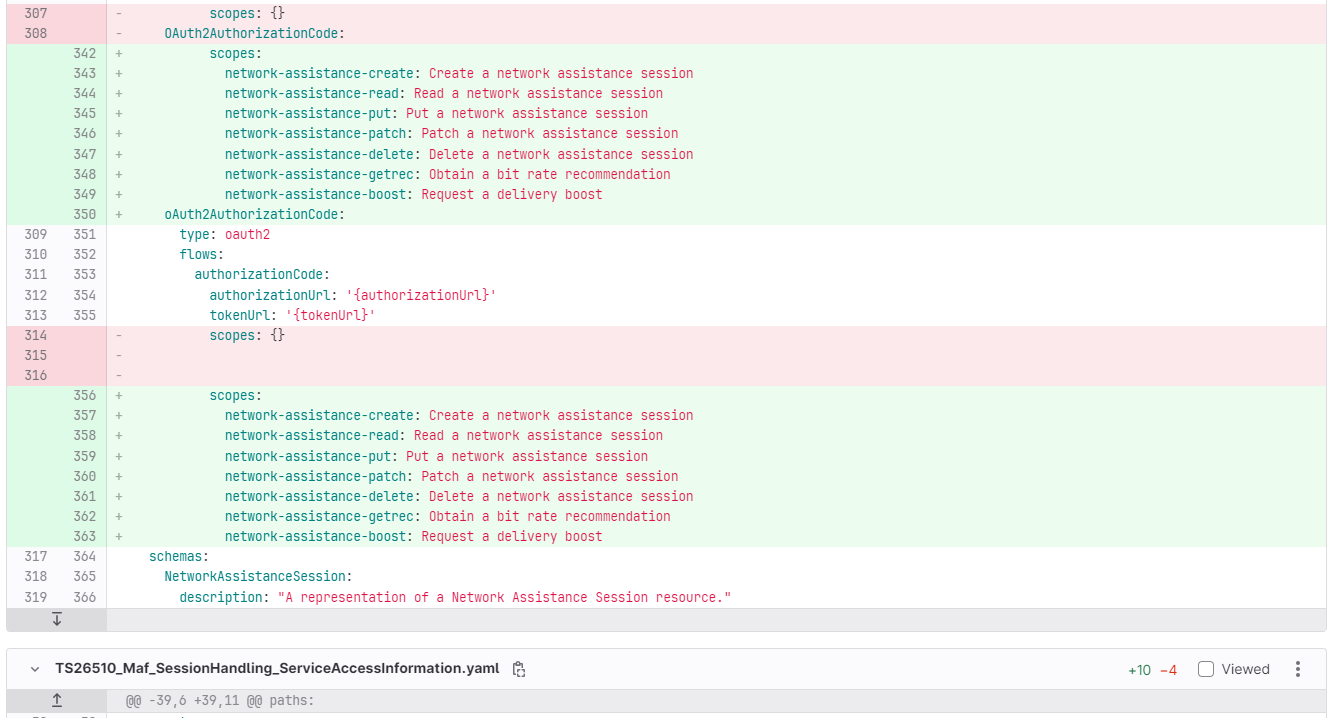


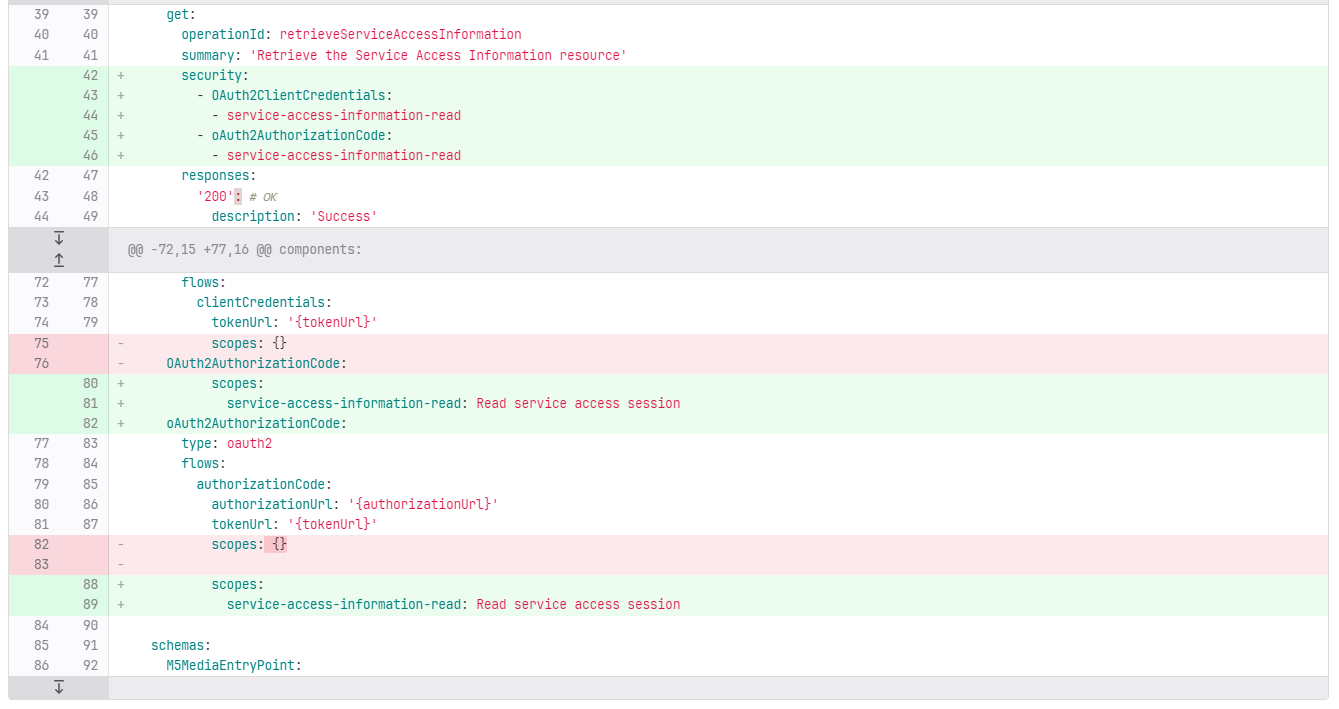


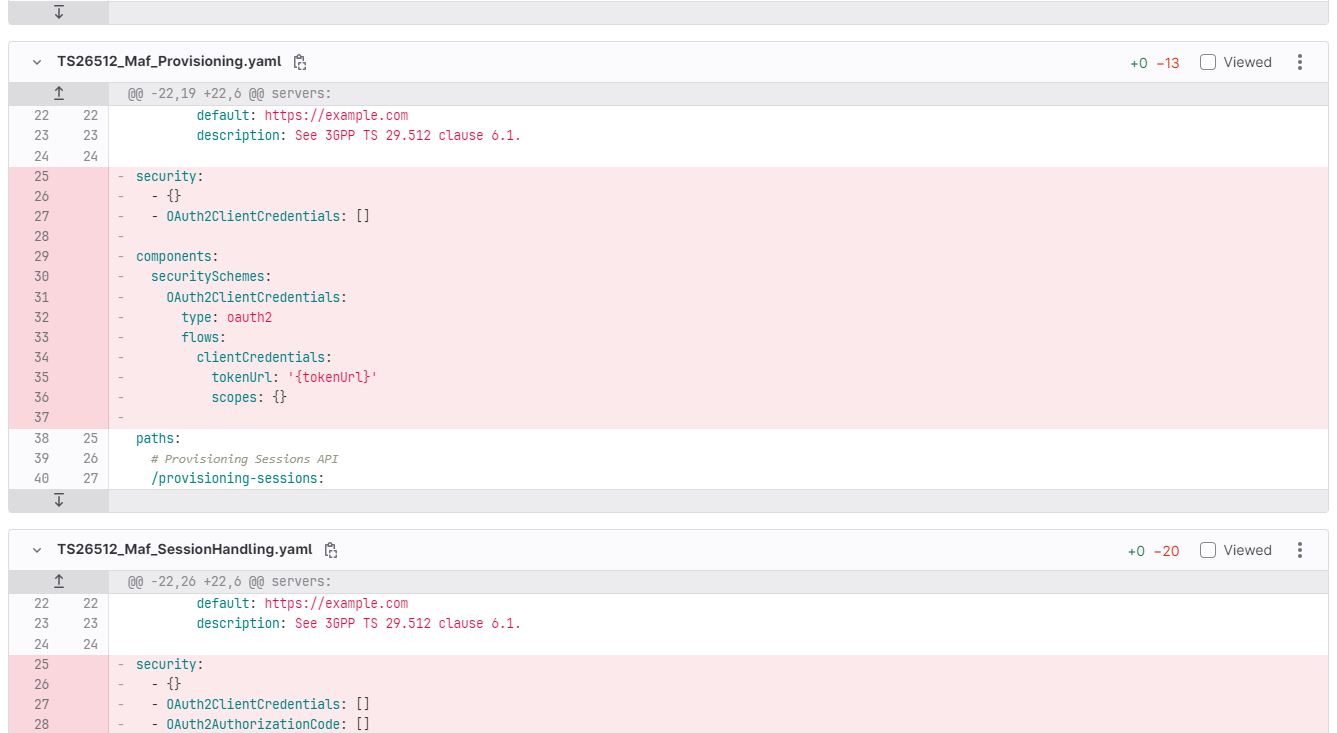














\*\*\*\* Last Change \*\*\*\*