**3GPP TSG- Meeting # *S4-240676***

**,**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *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**:

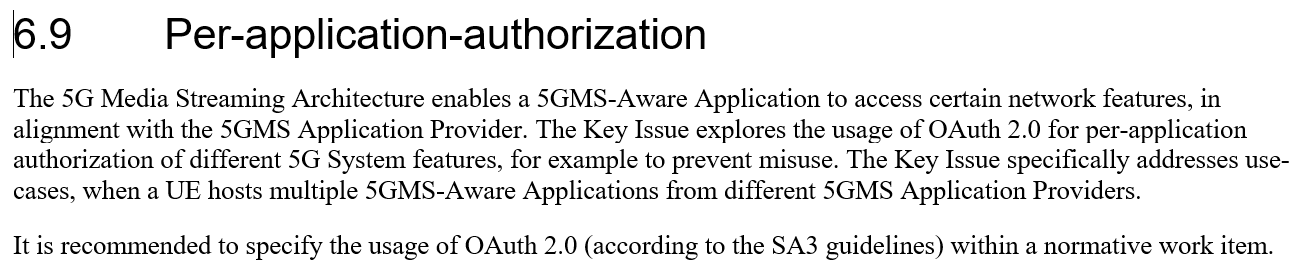
* Richard: Is the idea to obtain an authorization code, and use it subsequently in M5
* Thorsten: Yes
* Richard: Do we need this kind of security (oauth) at M5? Understand for M1. We got a security network right. What are you protecting against
* Thorsten: For example, you could have applications using 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.

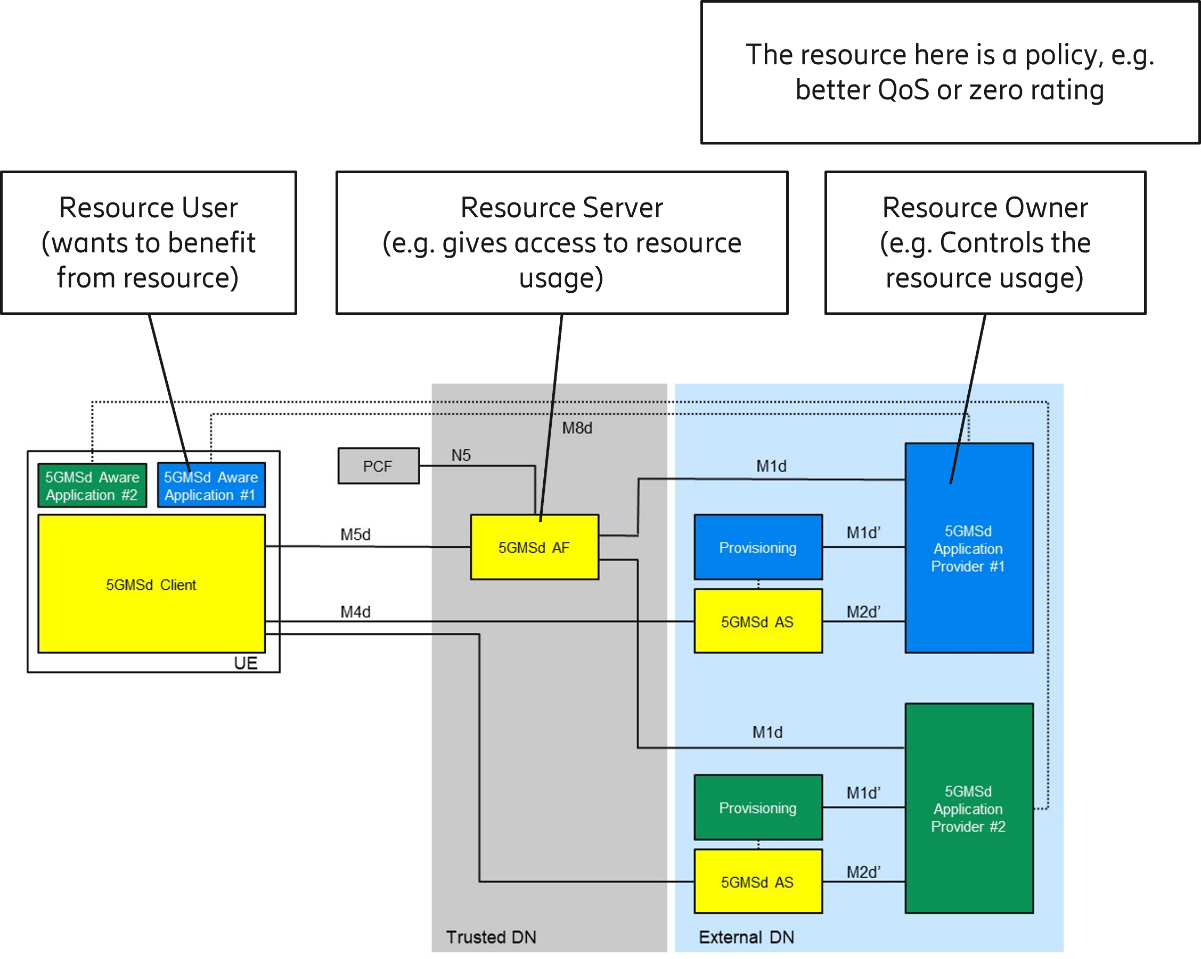


Figure 5.9.3-1: Applying roles for 5G Media Streaming Architecture functions

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.

• References are either specific (identified by date of publication, edition number, version number, etc.) or non specific.

• For a specific reference, subsequent revisions do not apply.

• For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[23502] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[26501] 3GPP TS 26.501: "5G Media Streaming (5GMS); General description and architecture".

[26506] 3GPP TS 26.506: "5G Real-time Media Communication Architecture (Stage 2)".

[26512] 3GPP TS 26.512: "5G Media Streaming (5GMS); Protocols".

[26113] 3GPP TS 23.113: "Real-Time Media Communication; Protocols and APIs".

[26247] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS); Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

[29122] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[X.509] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005: "Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".

[RFC5280] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.

[RFC7468] IETF RFC 7468: "Textual Encodings of PKIX, PKCS, and CMS Structures", April 2015.

[23558] 3GPP TS 23.558: "Architecture for enabling edge applications".

[24558] 3GPP TS 24.558: "Enabling Edge Applications; Protocol specification".

[29558] 3GPP TS 29.558: "Enabling Edge Applications; Application Programming Interface (API) specification; Stage 3".

[23503] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[23003] 3GPP TS 23.003: "Numbering, addressing and identification".

[29514] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[29522] 3GPP TS 29.522: "5G System. Network Exposure Function Northbound APIs; Stage 3".

[27007] 3GPP TS 27.007: "AT Command set for User Equipment (UE)".

[38321] 3GPP TS 38.321: "NR; Medium Access Control (MAC) protocol specification".

[36321] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".

[HTTPsemantics] IETF RFC 9110: "HTTP Semantics", June 2022.

[HTTPcaching] IETF RFC 9111: "HTTP Caching", June 2022.

[HTTP11] IETF RFC 9112: "HTTP/1.1", June 2022.

[HTTP2] IETF RFC 9113: "HTTP/2", June 2022.

[HTTP3] Reserved for future use.

[TLS13] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3", August 2018.

[29500] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[29501] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[OpenAPI300] OpenAPI: "OpenAPI 3.0.0 Specification", https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md.

[29571] 3GPP TS 29.571: "Common Data Types for Service Based Interfaces; Stage 3".

[RFC3339] IETF RFC 3339: "Date and Time on the Internet: Timestamps", July 2002.

[RFC3986] IETF RFC 3986: "URI Generic Syntax".

[ECMA262] Standard ECMA-262, 5.1 Edition: "ECMAScript Language Specification", June 2011.

[JSON] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format", December 2017.

[JSONSchema] IETF draft-bhutton-json-schema-validation: "JSON Schema Validation: A Vocabulary for Structural Validation of JSON", June 2022.

[26118] 3GPP TS 26.118: "Virtual Reality (VR) profiles for streaming applications".

[29517] 3GPP TS 29.517: "5G System; Application Function Event Exposure Service; Stage 3".

[26532] 3GPP TS 26.532: "Data Collection and Reporting; Protocols and Formats".

[26346] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[26347] 3GPP TS 26.347: "Multimedia Broadcast/Multicast Service (MBMS); Application Programming Interface and URL".

[ISO3166-1] ISO 3166 1: "Codes for the representation of names of countries and their subdivisions — Part 1: Country codes".

[ISO3166-2] ISO 3166 2: "Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code".

[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: "OAuth2.0 Authorization Framework".

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

[33501] 3GPP TS 33.501: "Security architecture and procedures for 5G System"

[33122] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

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

## 7.4 Security

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

In the Media Delivery System, the Media AF securely exposes capabilities and events to Media Application Providers. The Media AF enable secure provision of information in the Media Delivery System by authenticated and authorized Media Applications or Media Application Provider functions.

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

When OAuth 2.0 [RFC6749] is used as the selected security method between the Media Application Provider and the Media AF:

- The Media Application Provider, prior to consuming services offered by the Maf\_Provisioning API, shall obtain an access token from the authorization server, by invoking the Obtain\_Authorization service, specified in clause 5.6.2.3.2 of TS 29.222 [29222].

As indicated in 3GPP TS 33.122 [33122], access to the Maf\_Provisioning API may be authorized by means of the OAuth 2.0 protocol (see IETF RFC 6749 [RFC6749]), using the "Client Credentials" authorization grant, where the CAPIF core function (see 3GPP TS 29.222 [29222]) plays the role of the authorization server.

When CAPIF is used for external exposure

- Before invoking the API exposed by the Media AF, the Media Application Provider as API invoker shall negotiate the security method (PKI, TLS-PSK or OAuth 2.0) with the CAPIF Core Function and ensure that the Media AF has required credential to authenticate 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 used as the selected security method between the Media Application Provider and the Media AF, upon API invocation, the Media AF shall retrieve the authorization information from the CAPIF core function as described in clause 5.6.2.4 of 3GPP TS 29.222 [29222],

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

Access to the Maf\_SessionHandling APIs of theMedia AF by the Media Session Handler at reference point M5 shall be authorised by means of OAuth2.0 Authorization Framework [RFC6749], using the "Client Credentials" or "Authorization Code" flow grant types.

Editor's Note: Awaiting contribution.

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

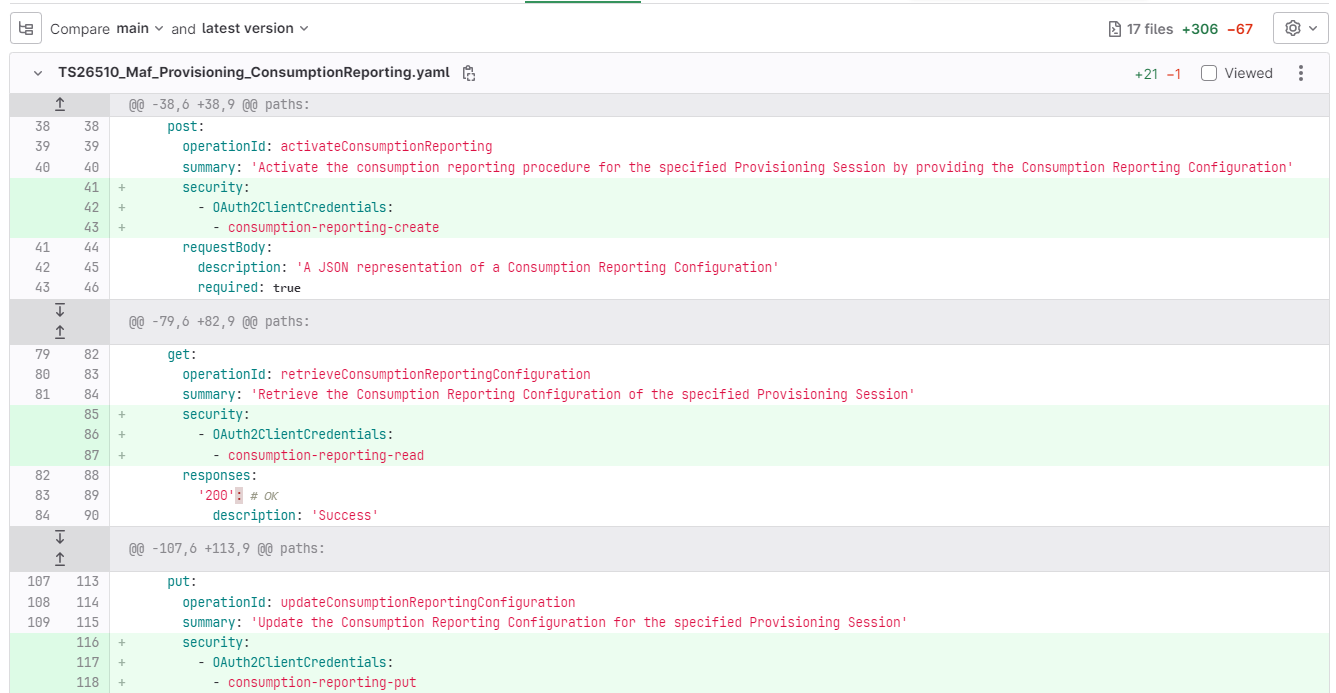
# 3GPP Forge merge request

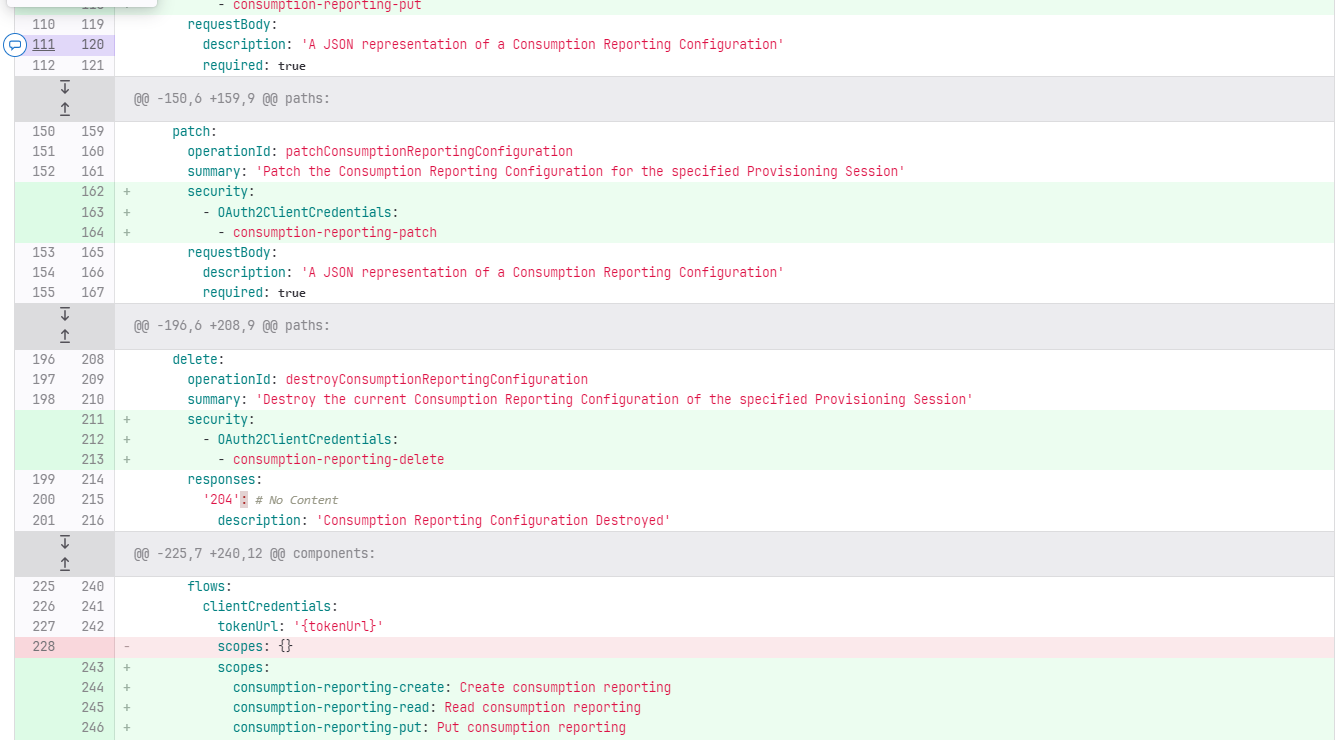
The code changes associated with this Change Request are available for review at the following URL:

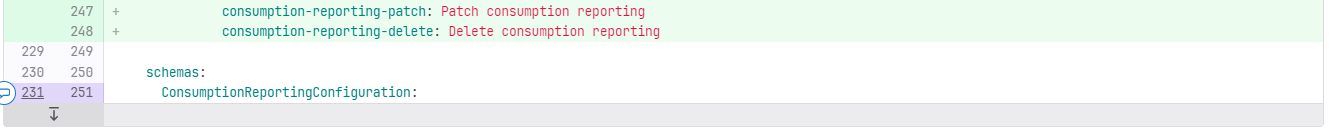
<https://forge.3gpp.org/rep/sa4/5gms_pro_ph2/-/merge_requests/6/diffs>

The proposed changes are reproduced below for posterity:

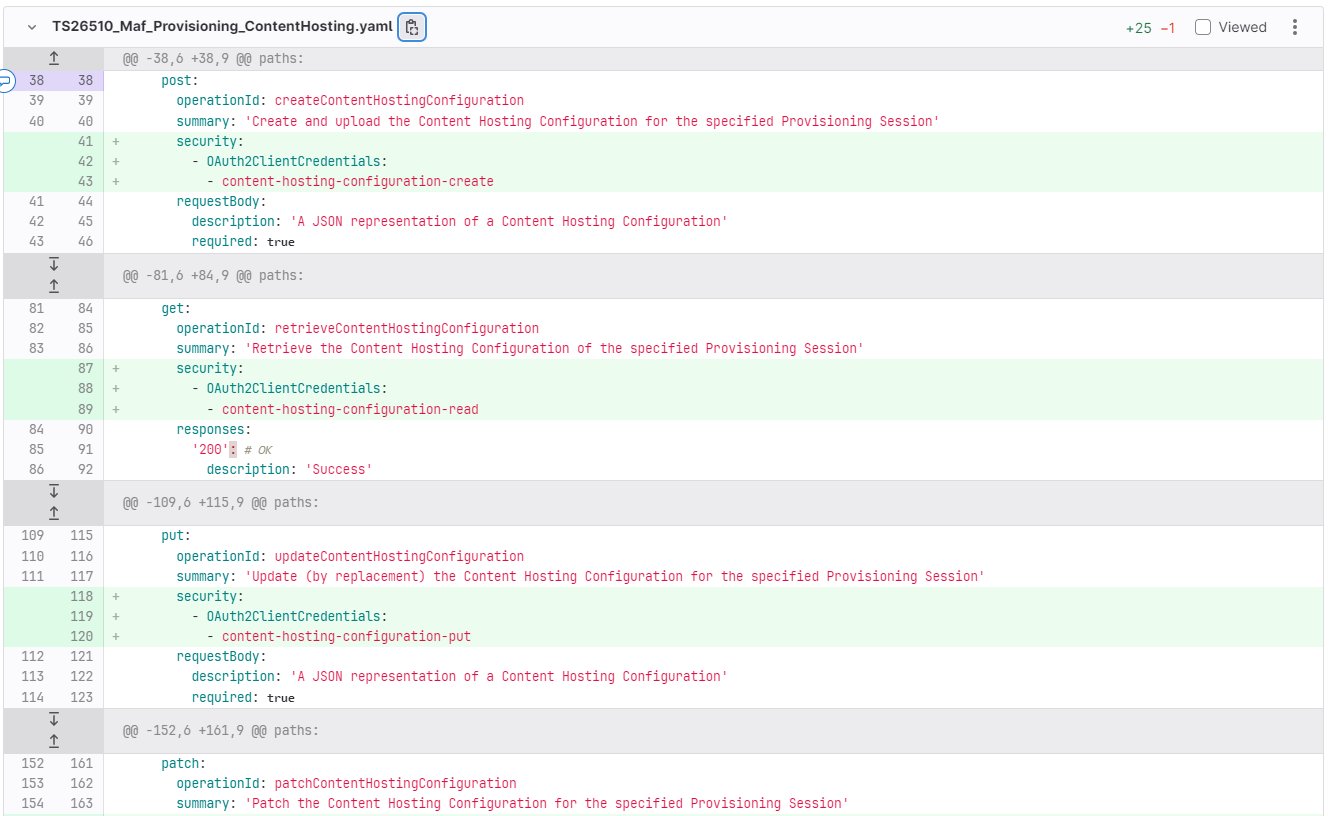
The OAuth 2.0 specific definitions follow [OAuth 2.0 (swagger.io)](https://swagger.io/docs/specification/authentication/oauth2/)

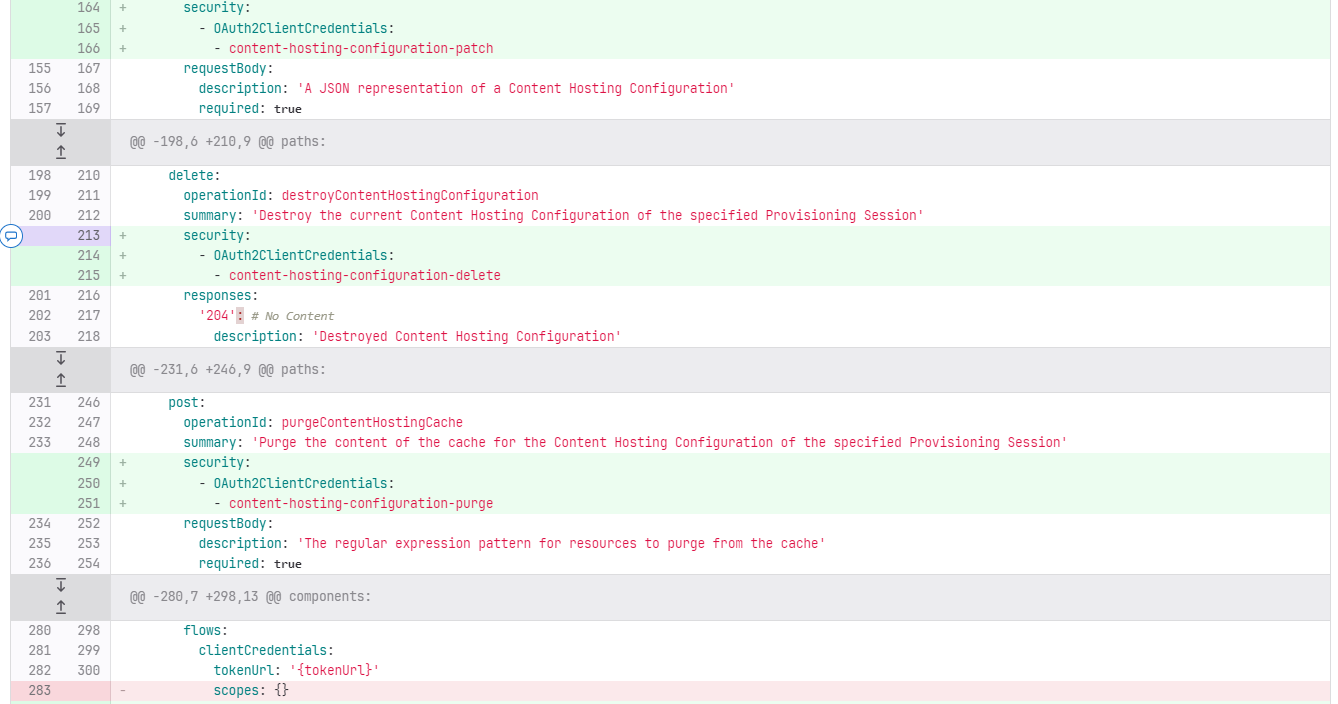


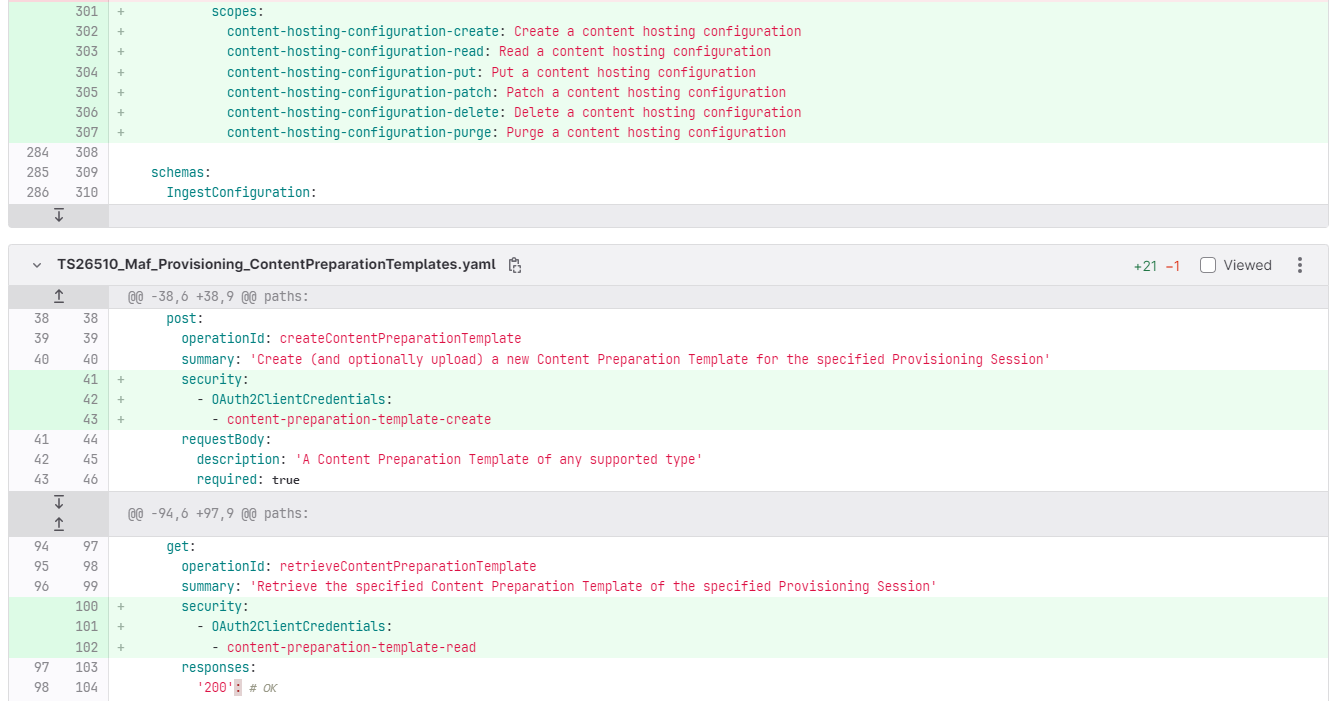


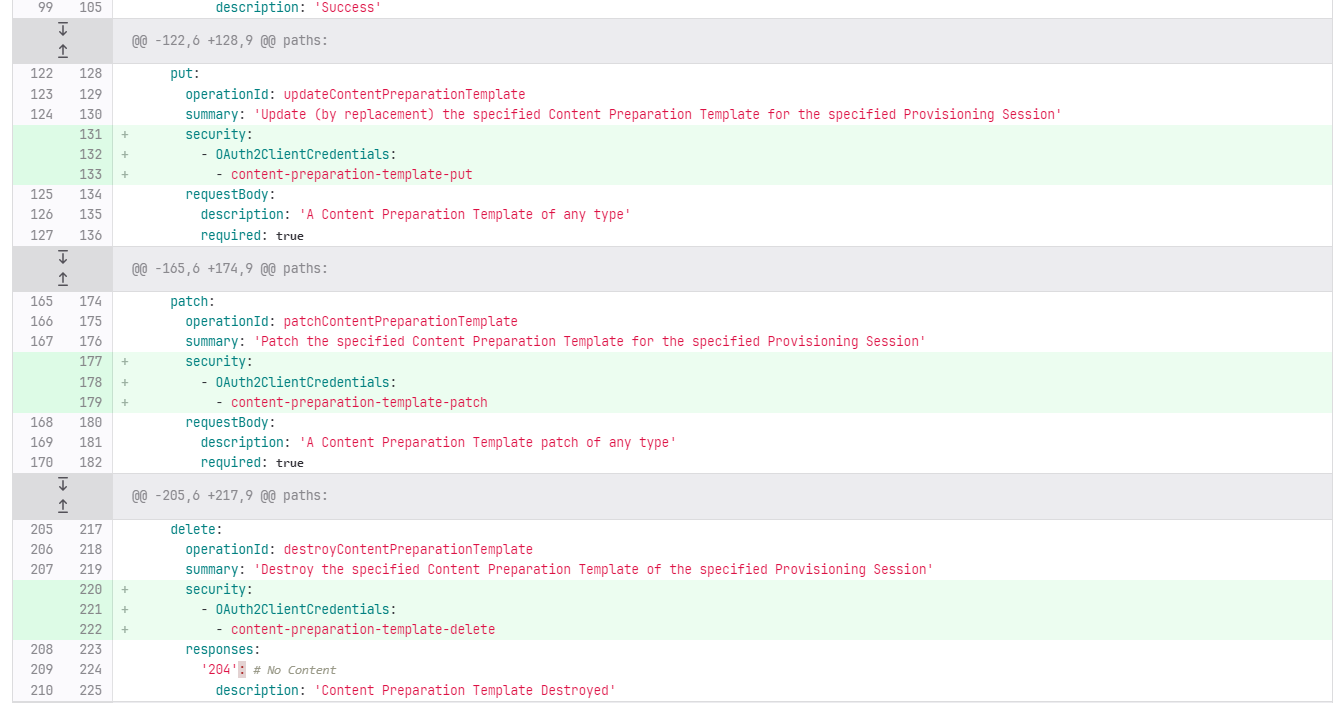


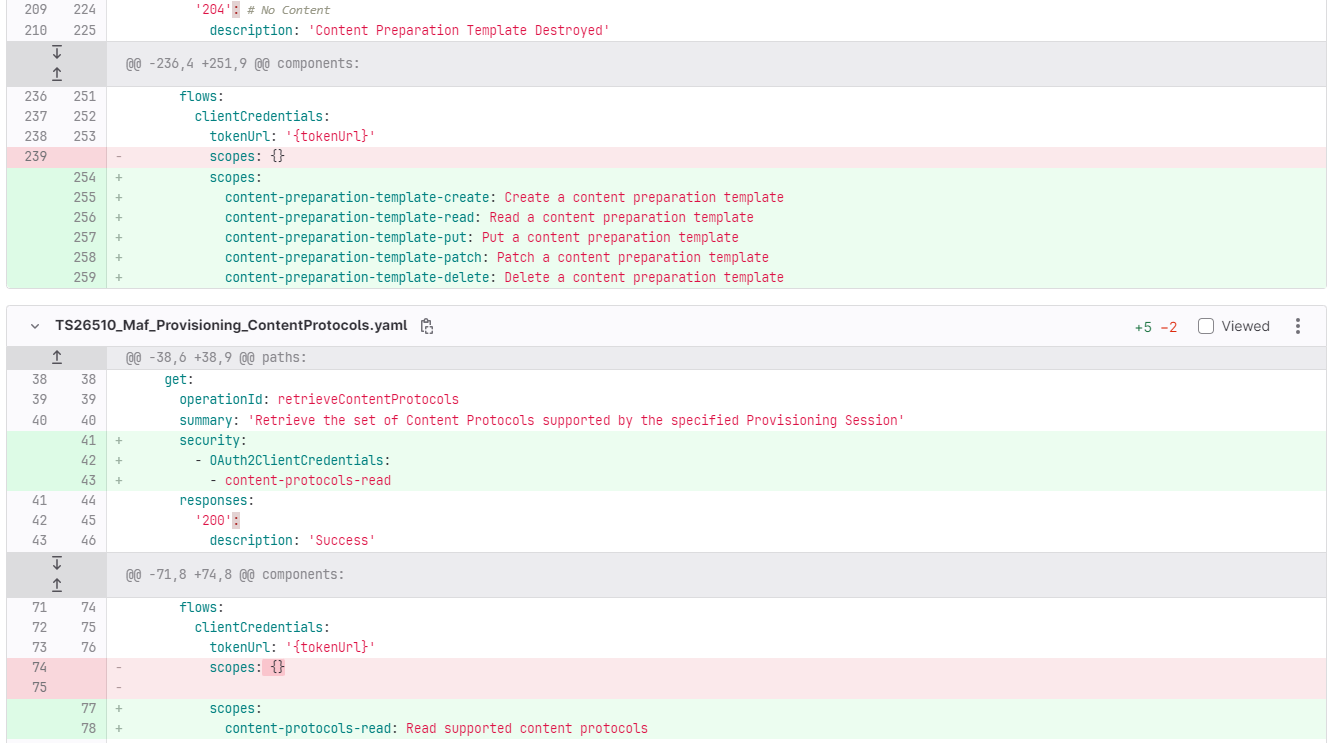
TS26510\_Maf\_Provisioning\_ContentHosting.yaml



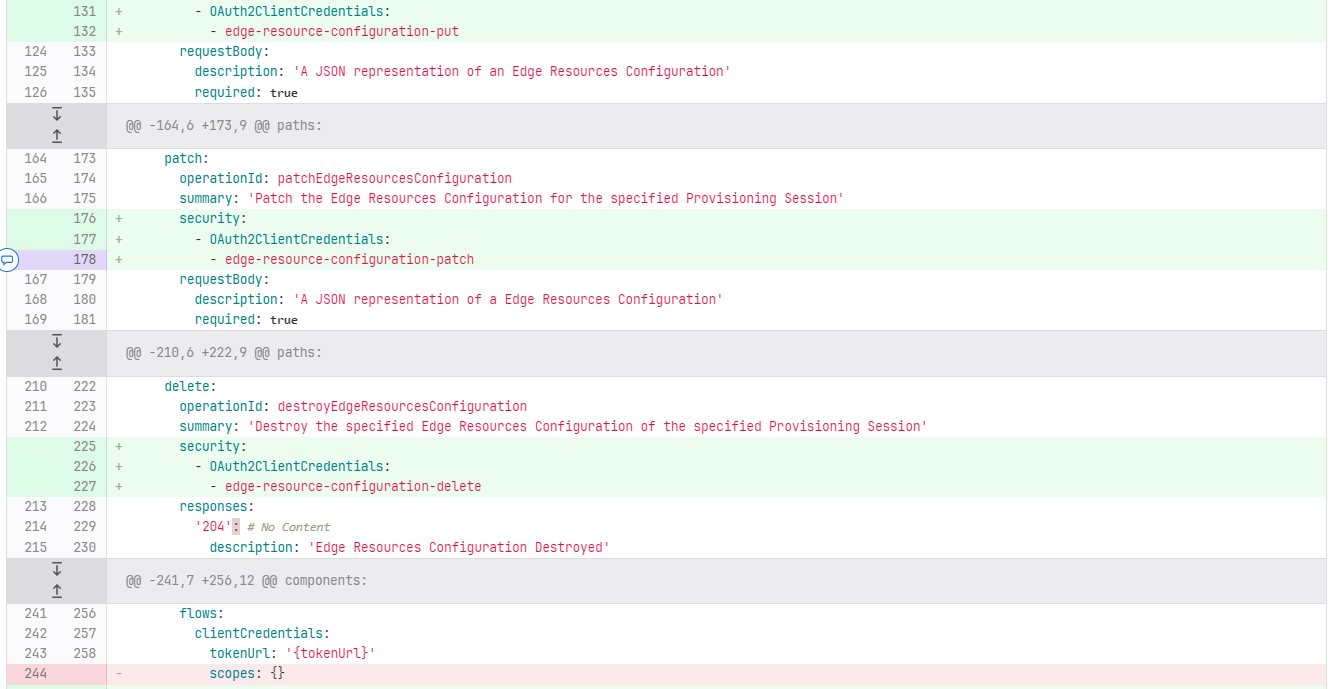


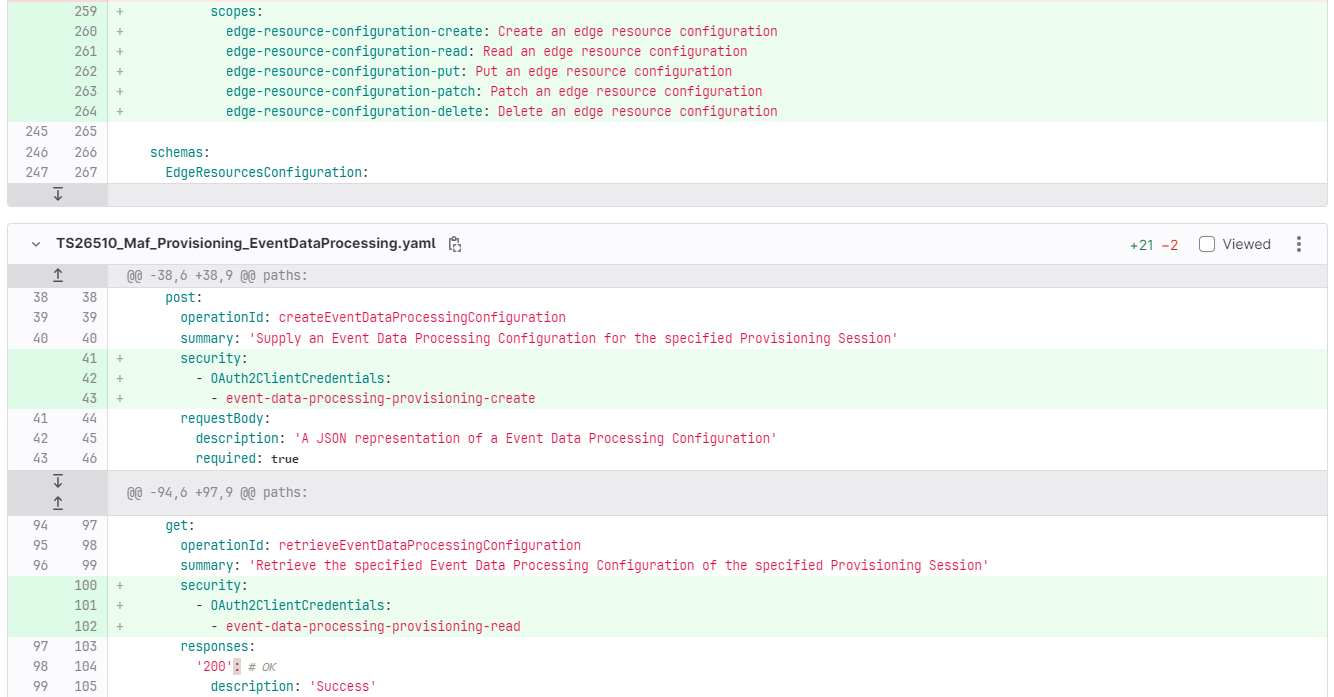




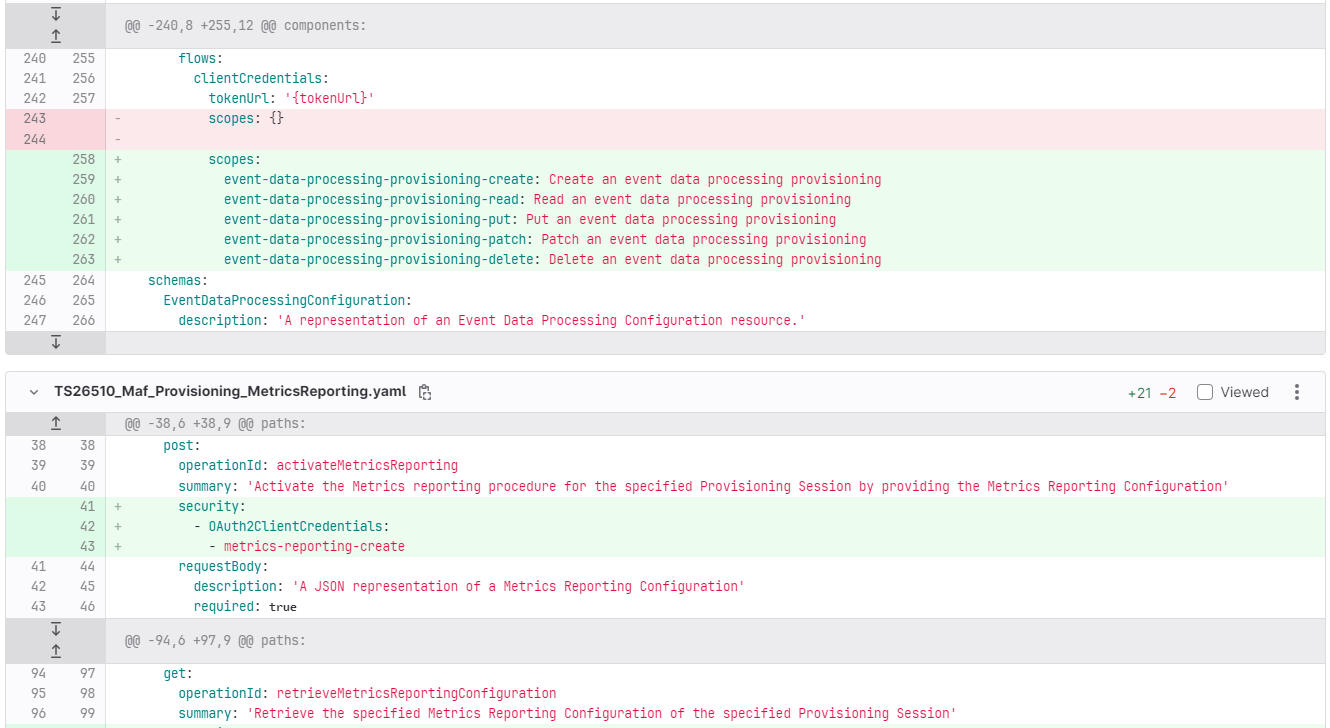


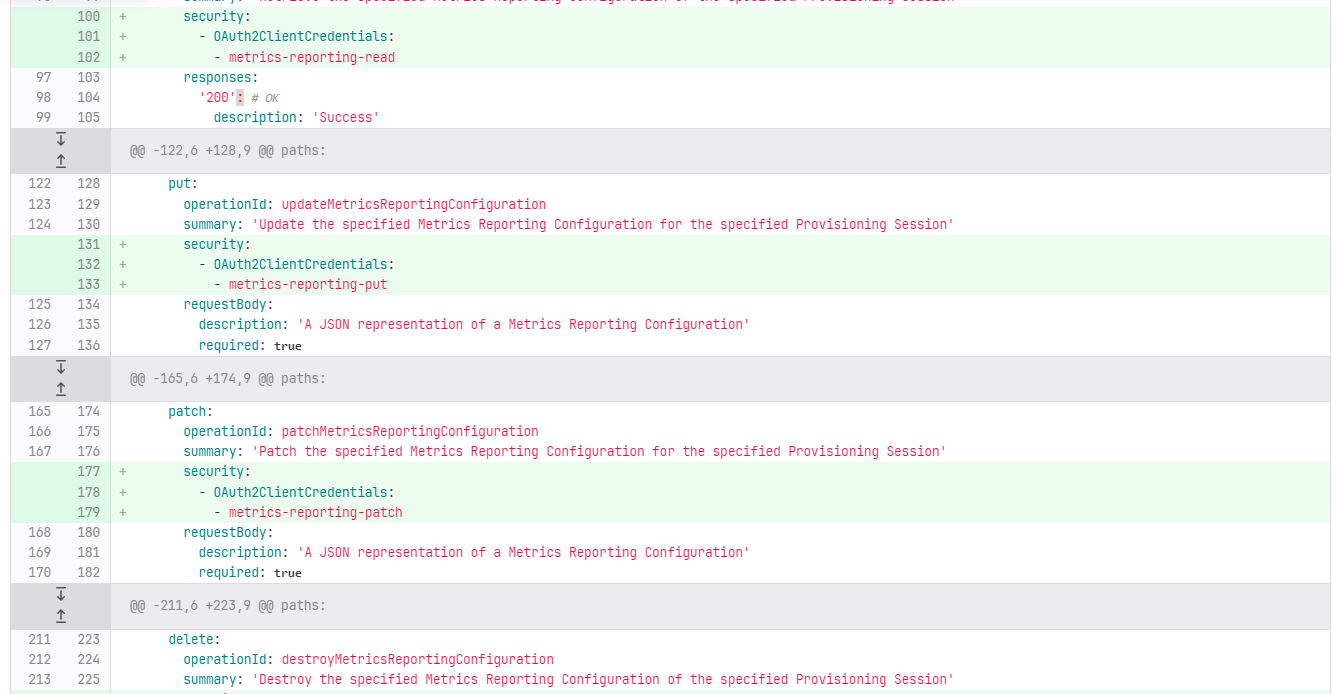


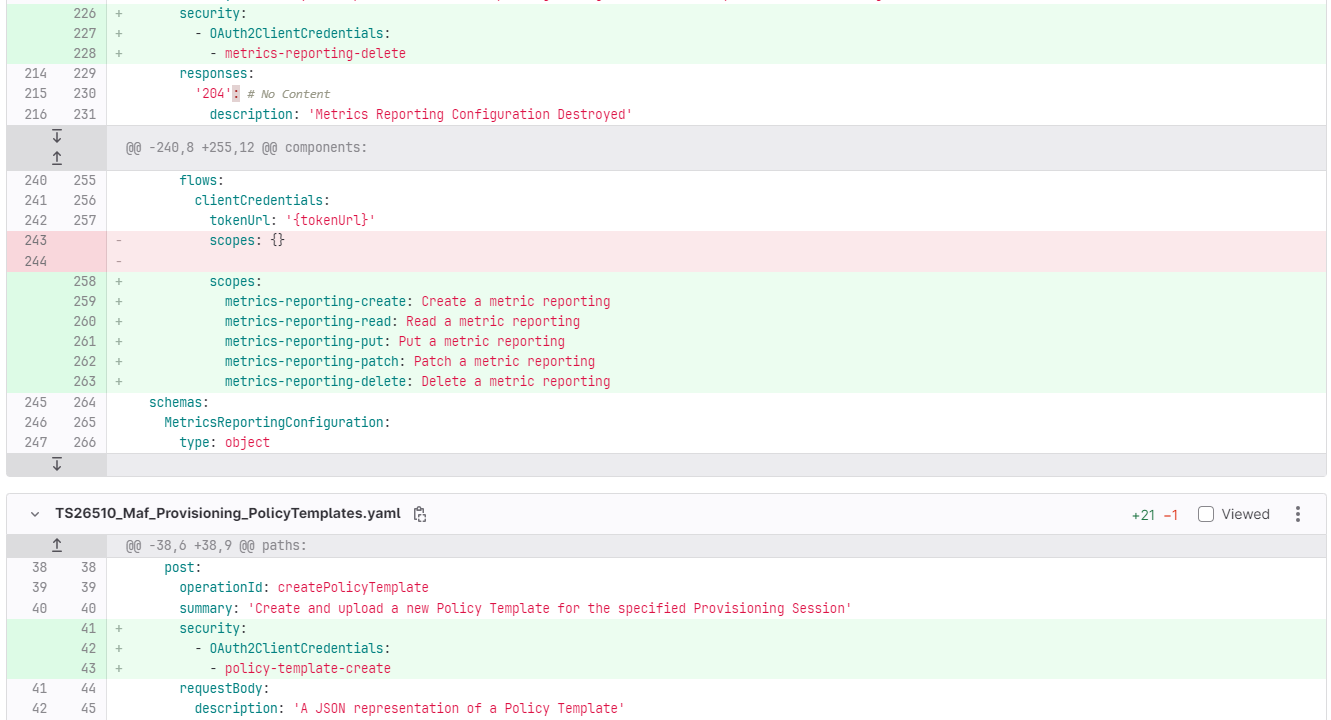


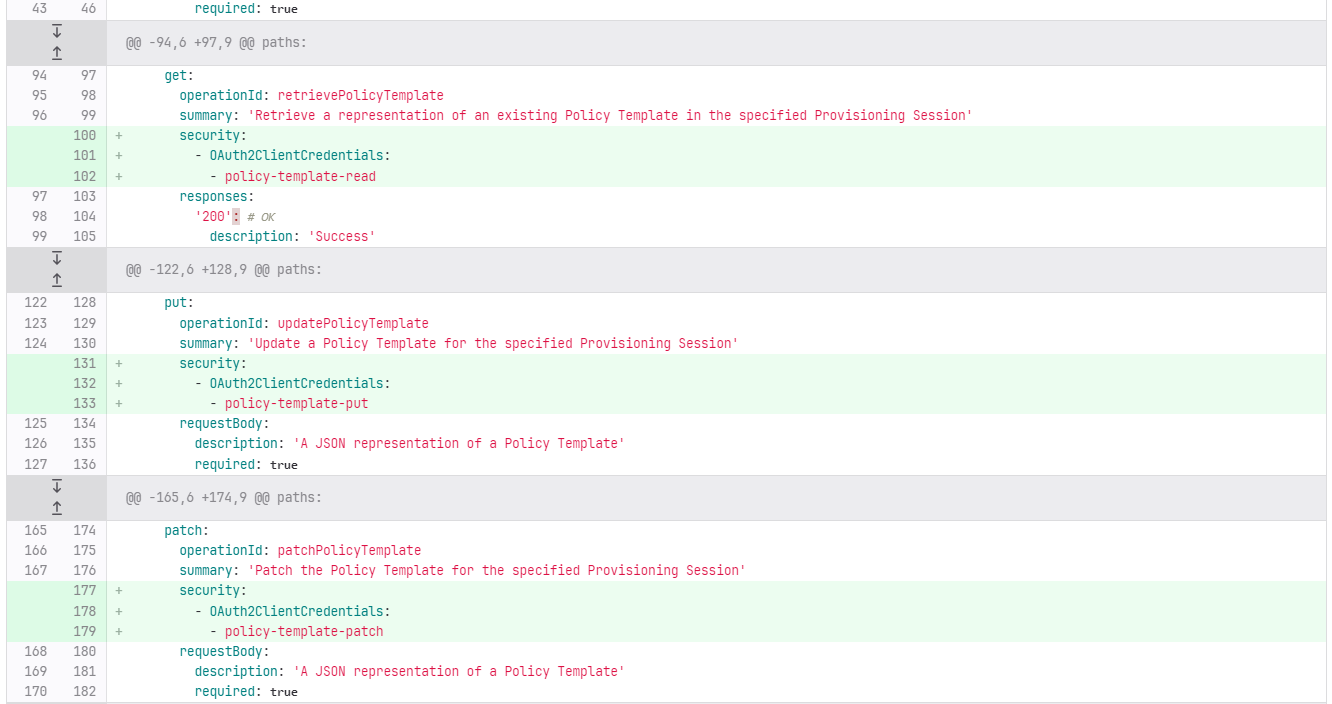


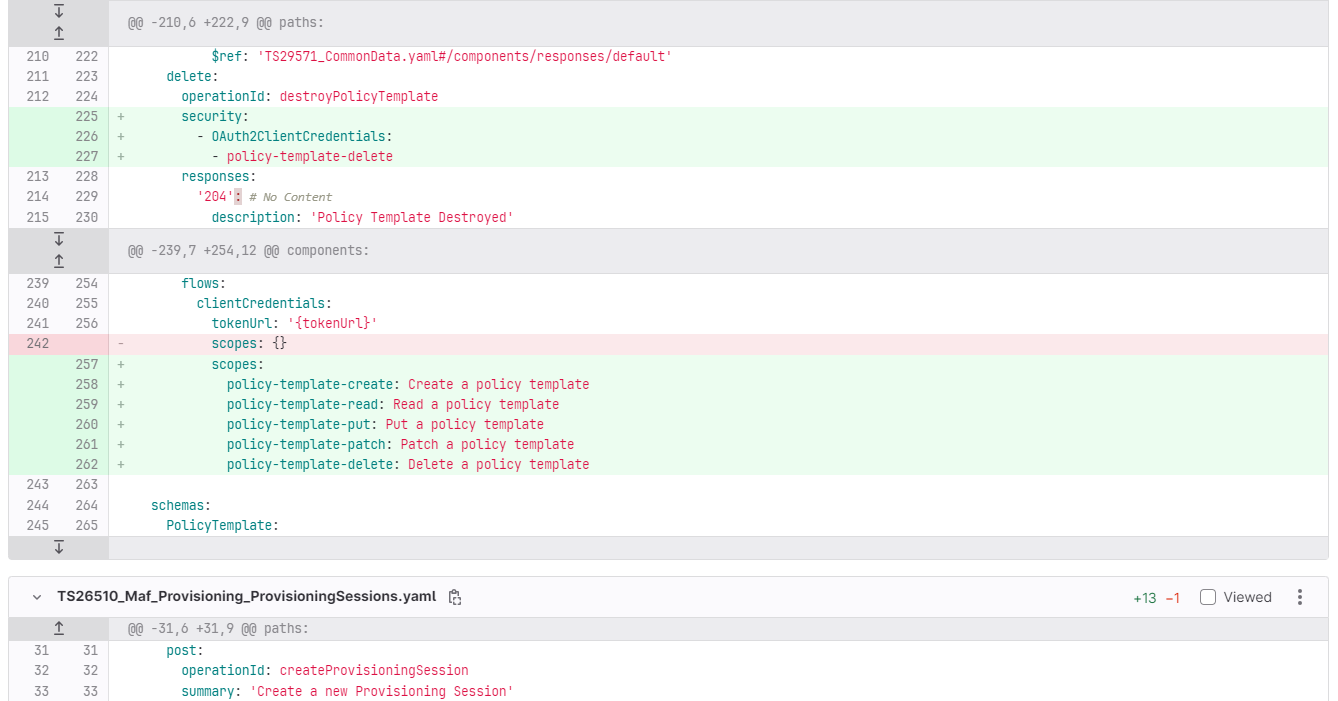


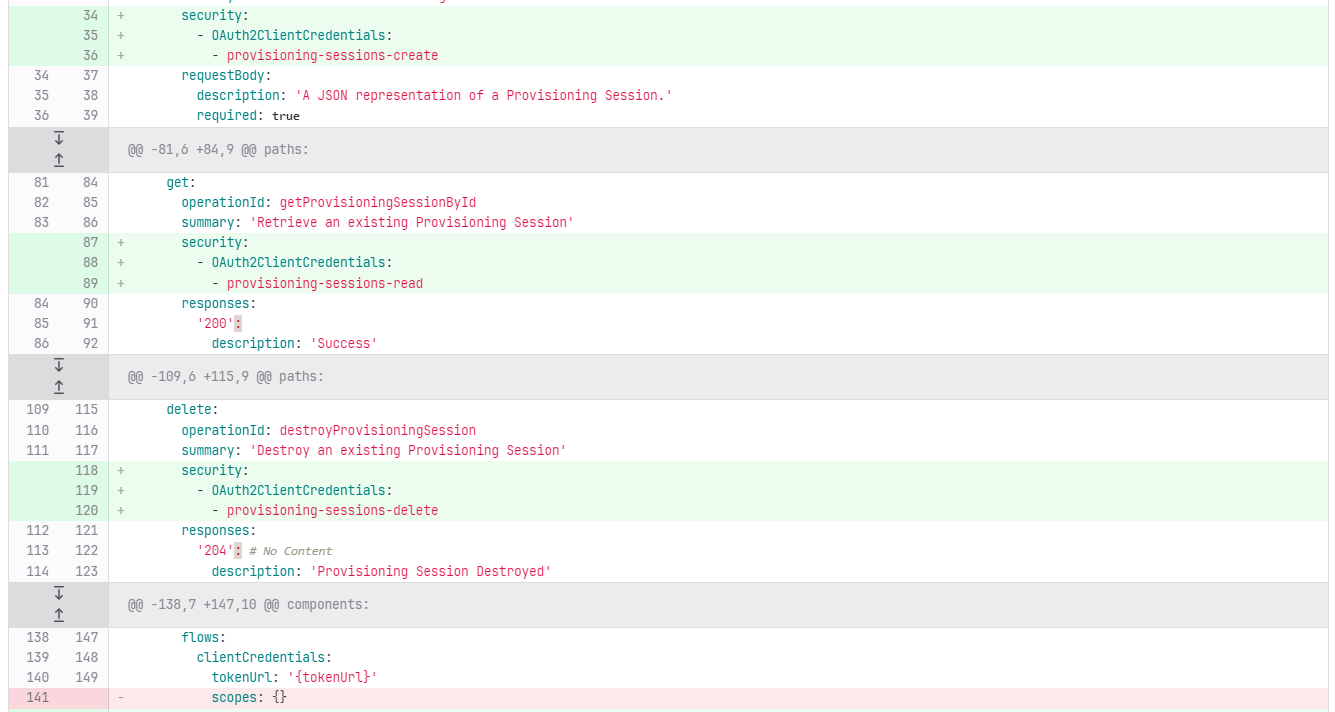




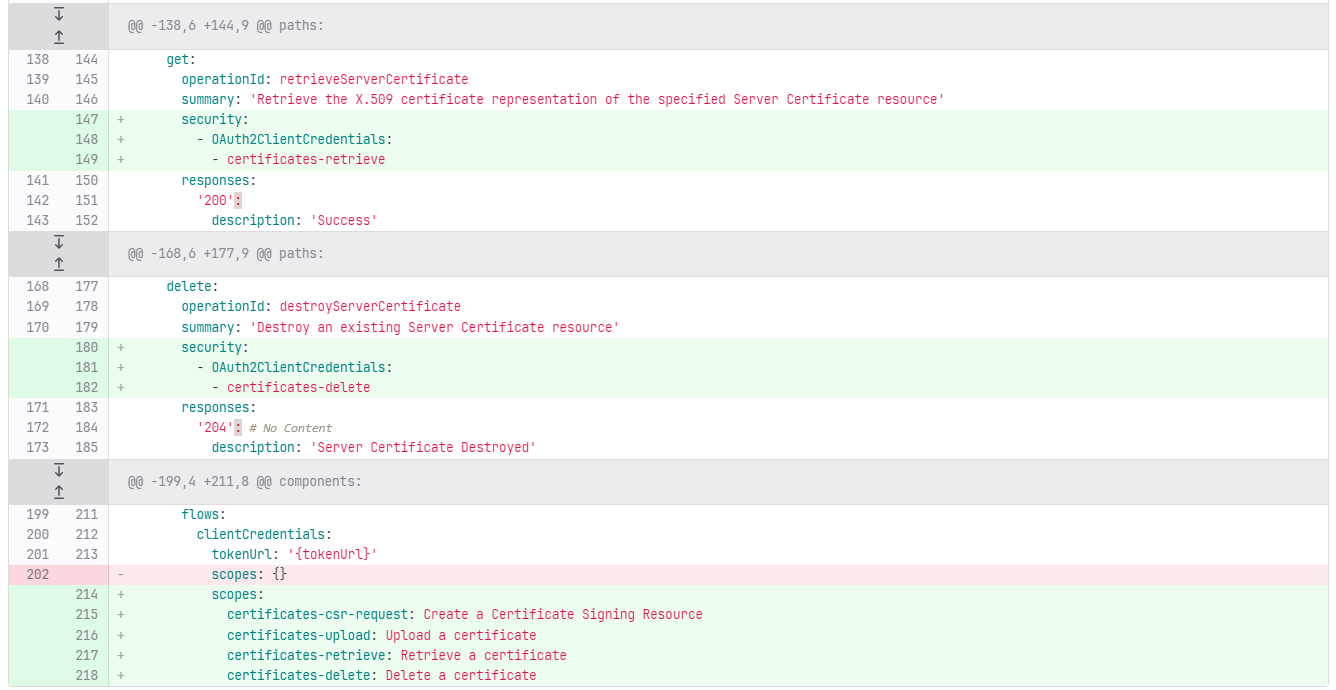


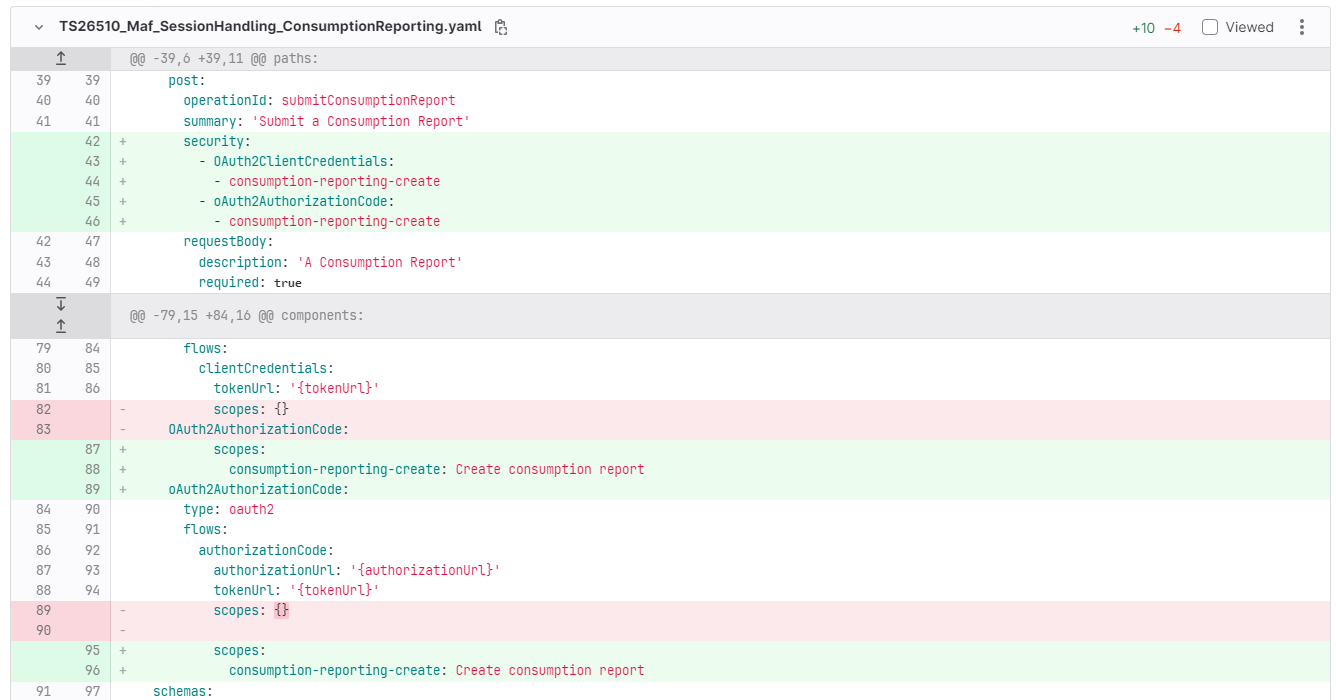


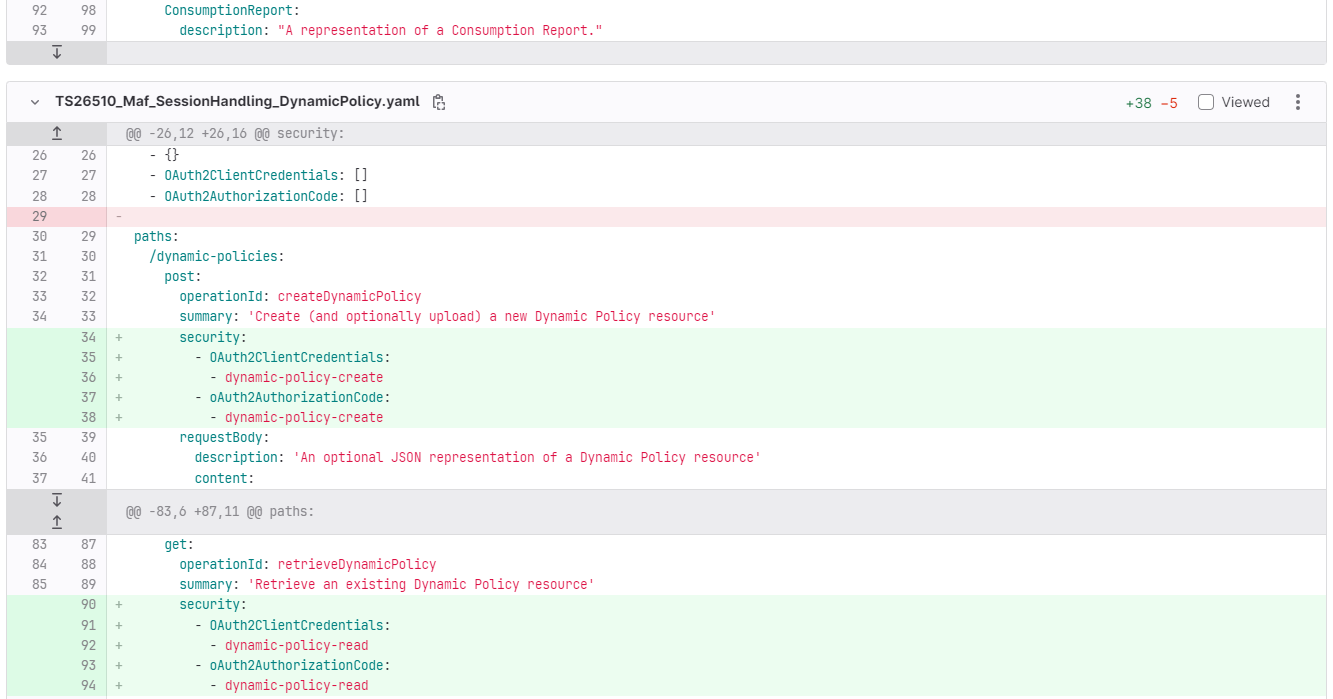


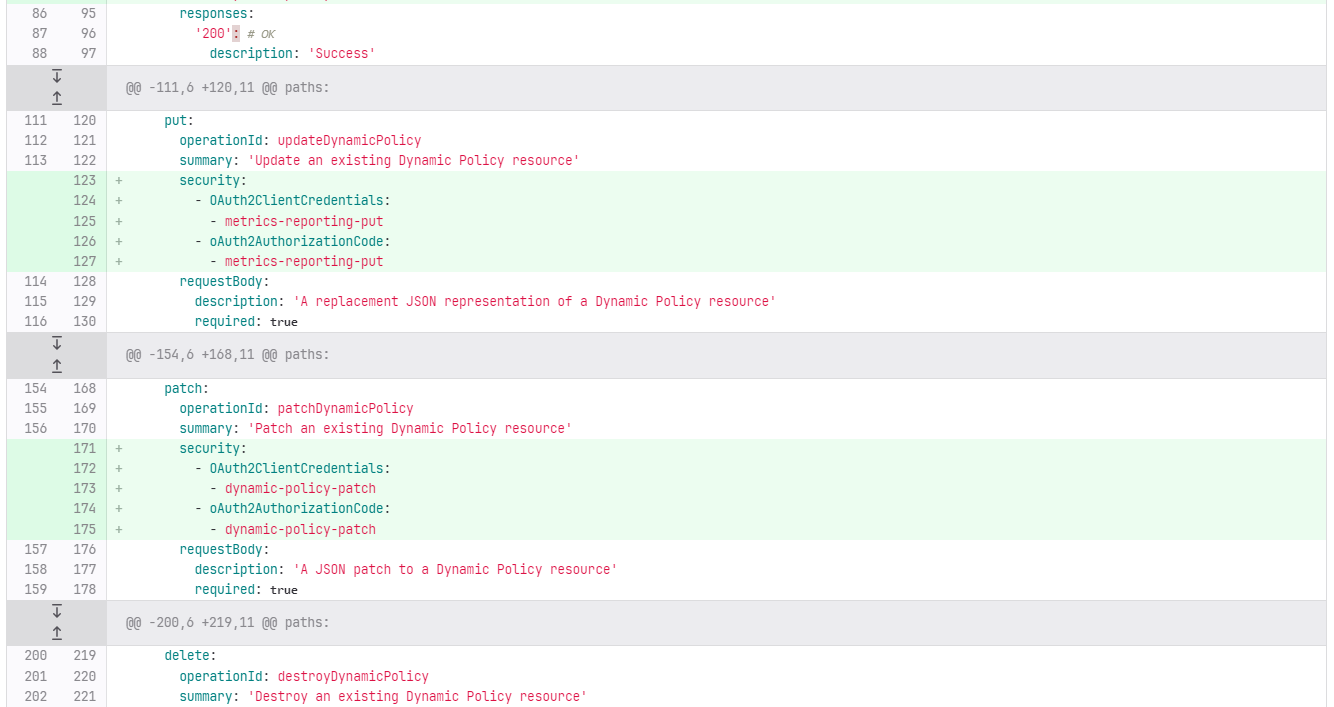


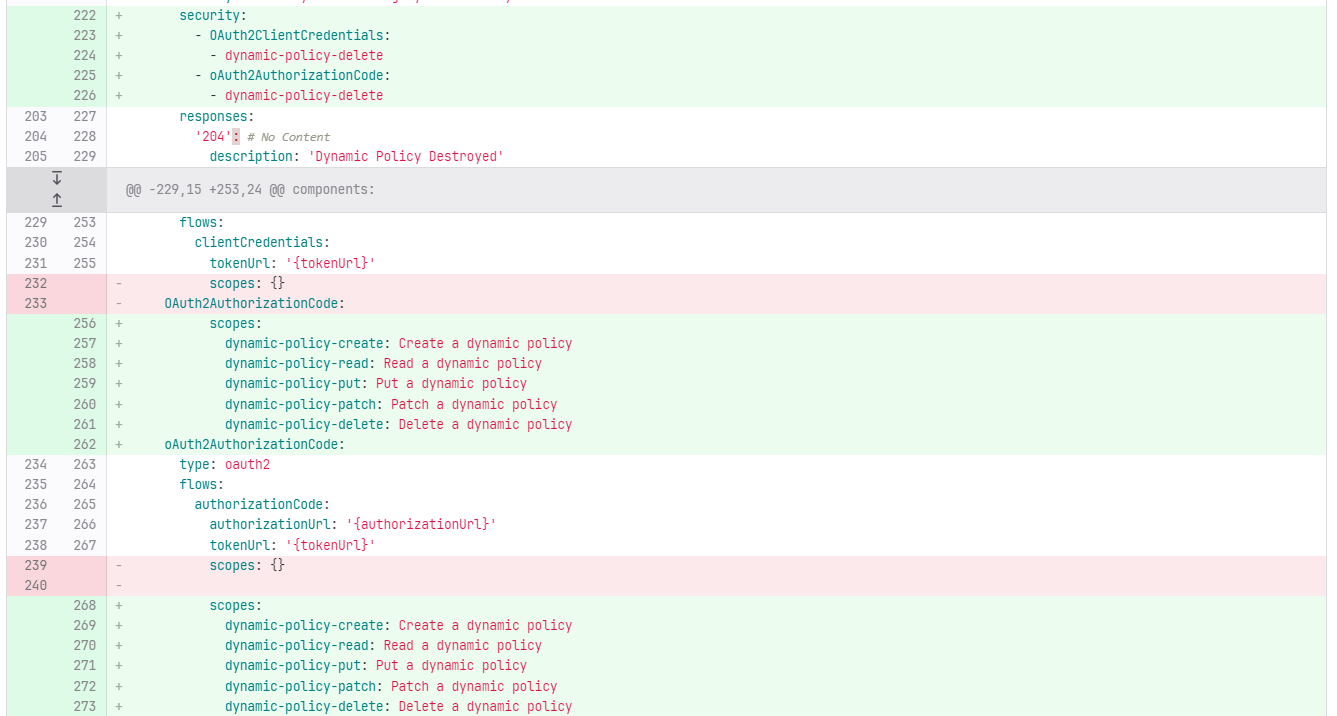


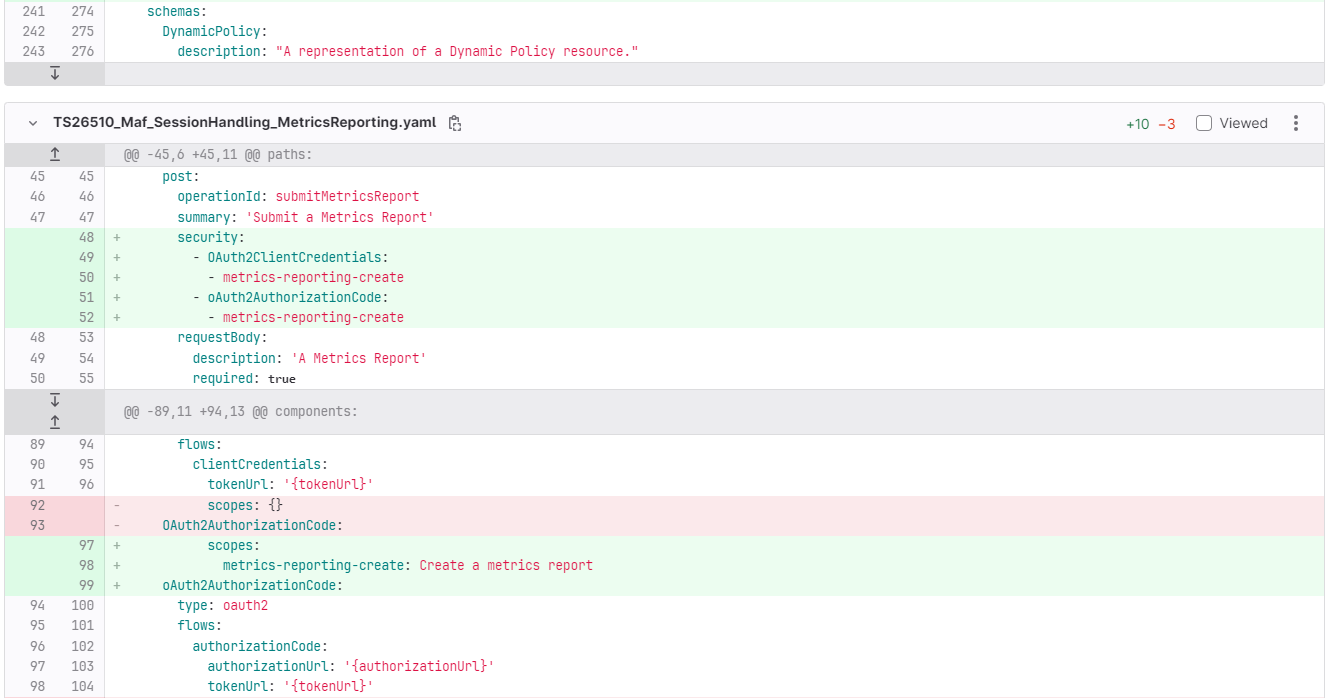


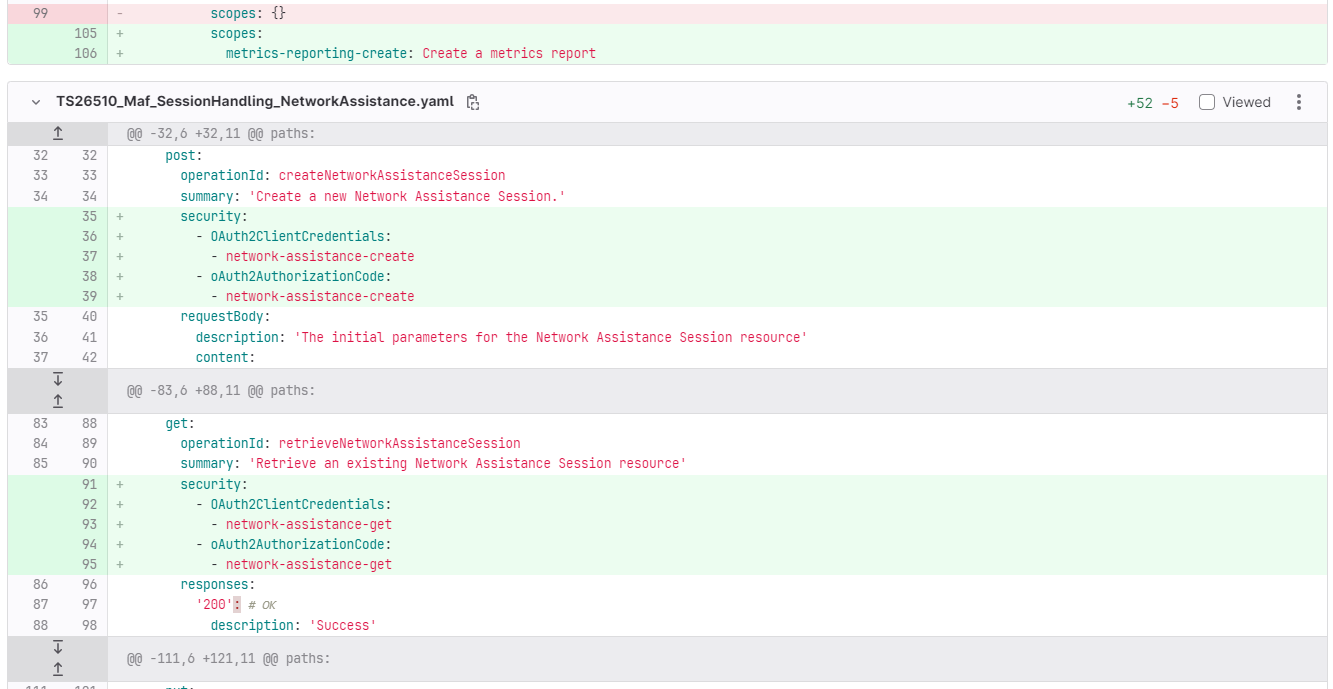


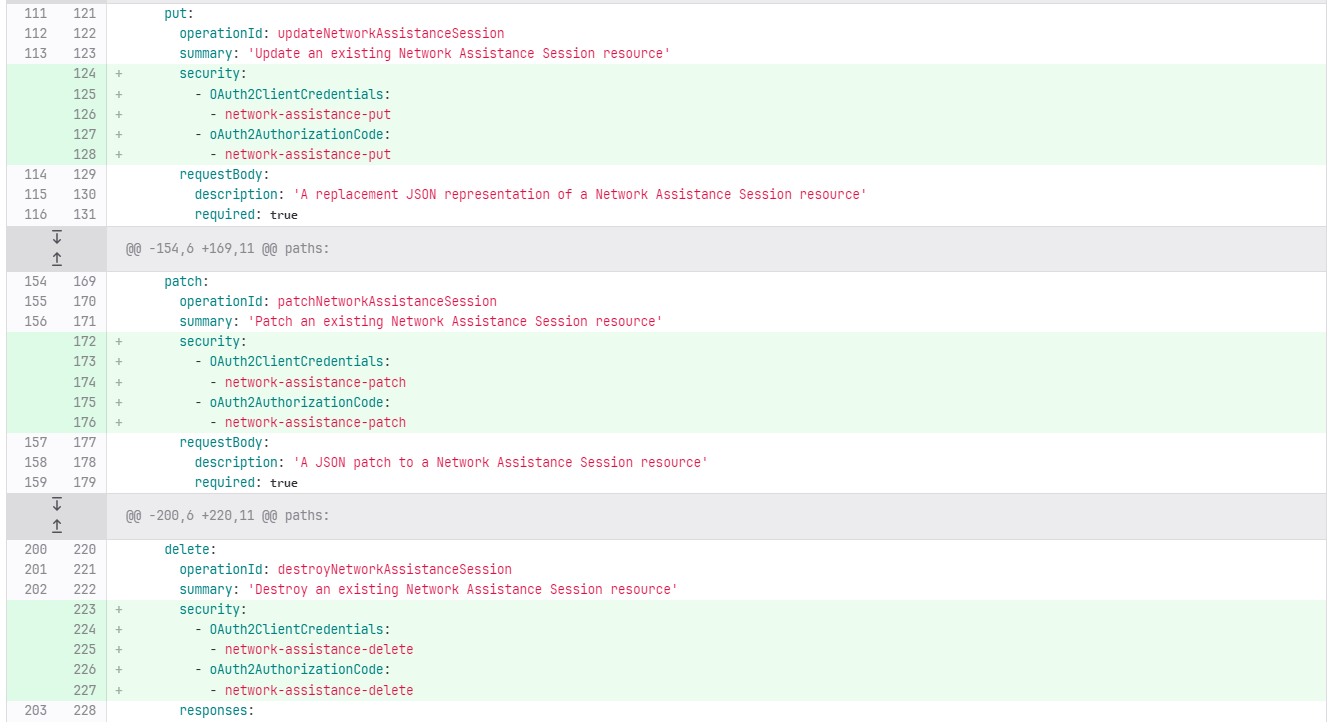


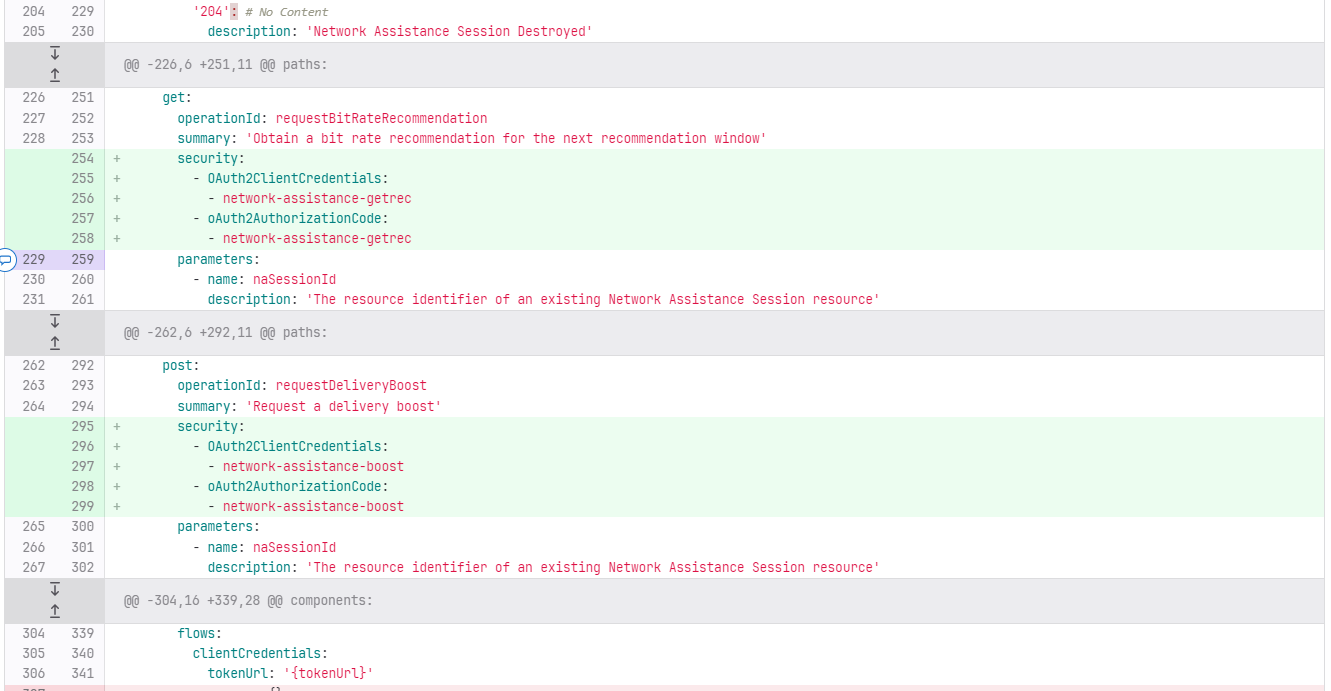


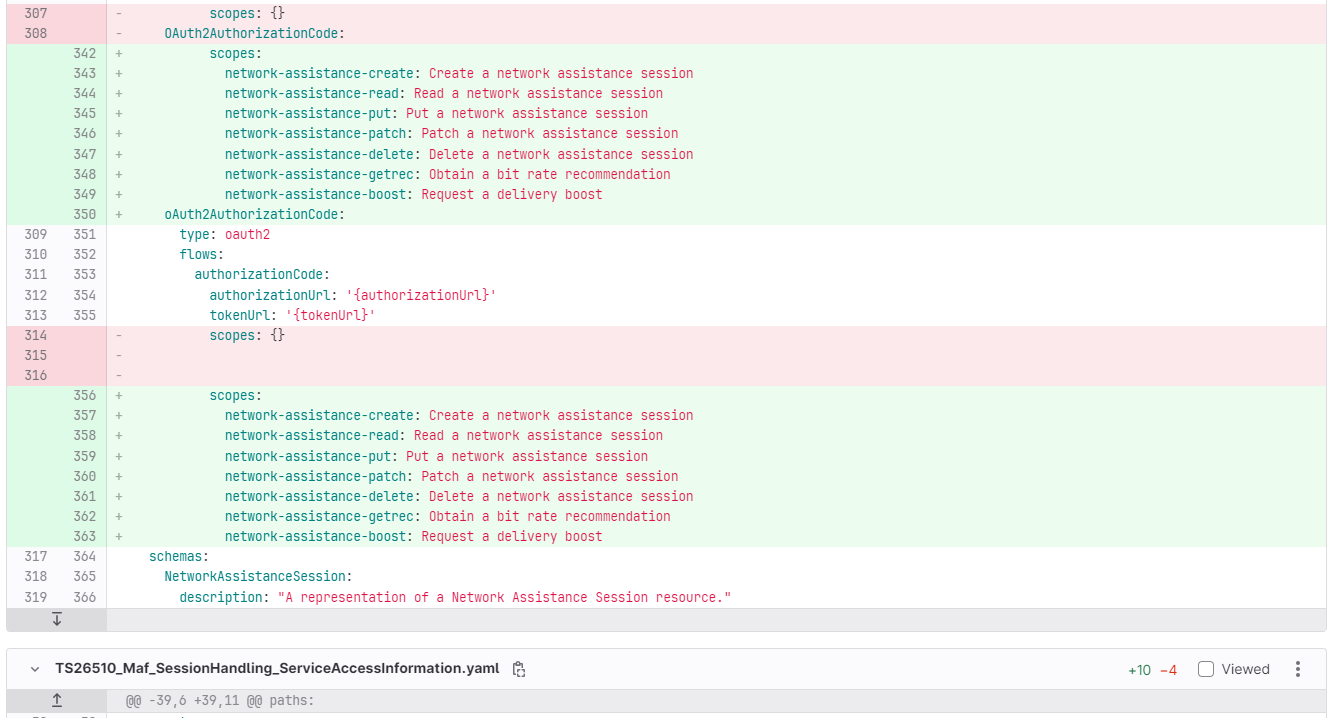


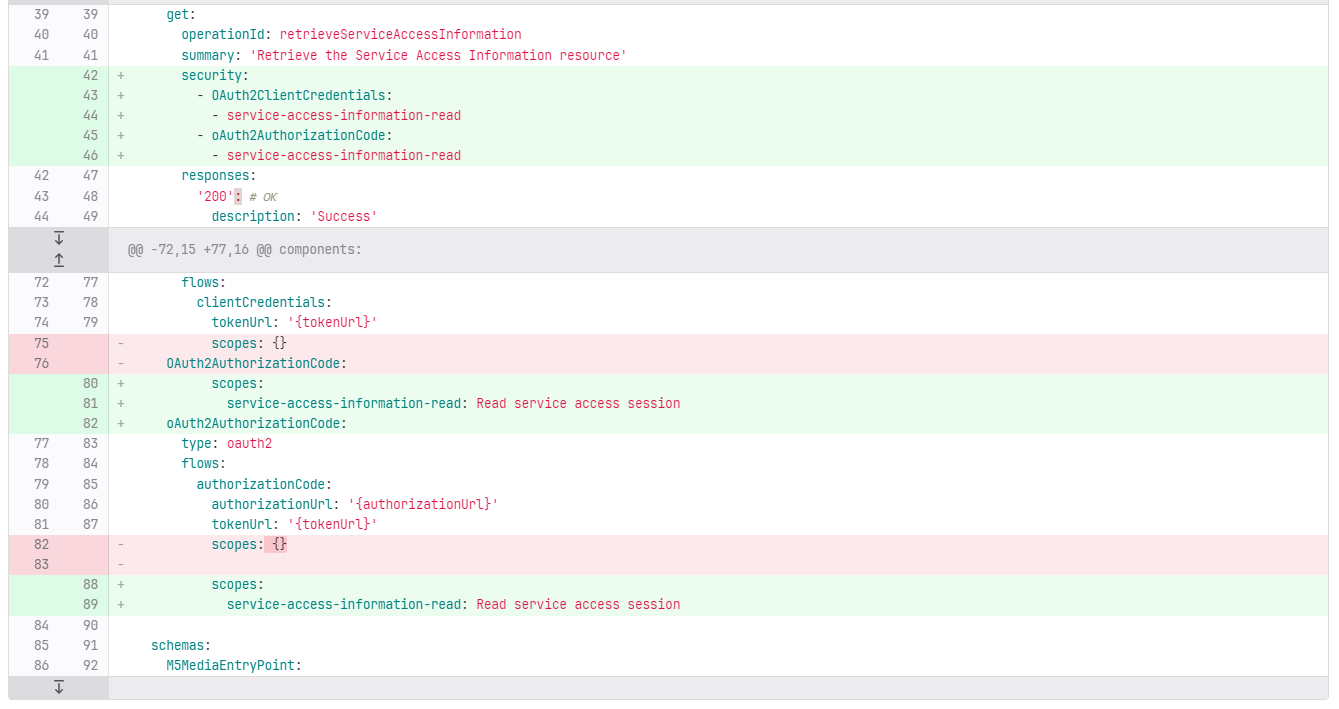


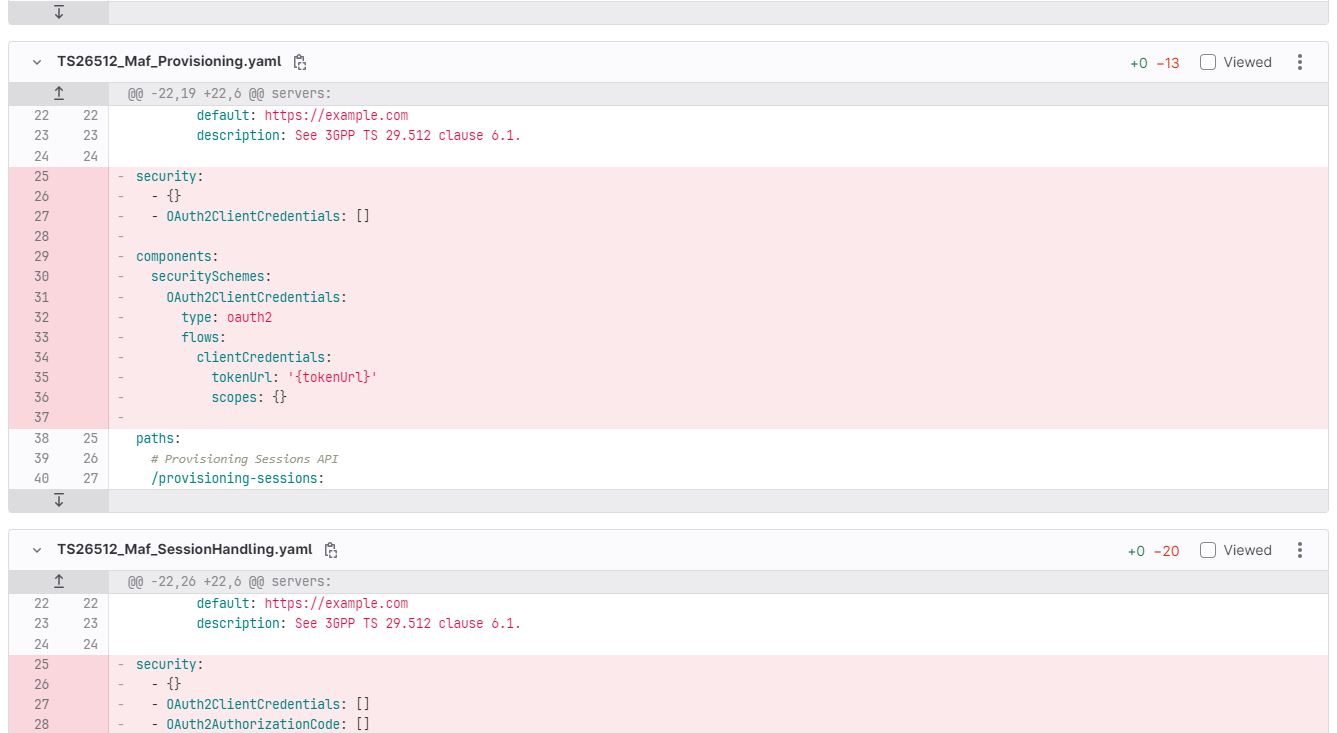


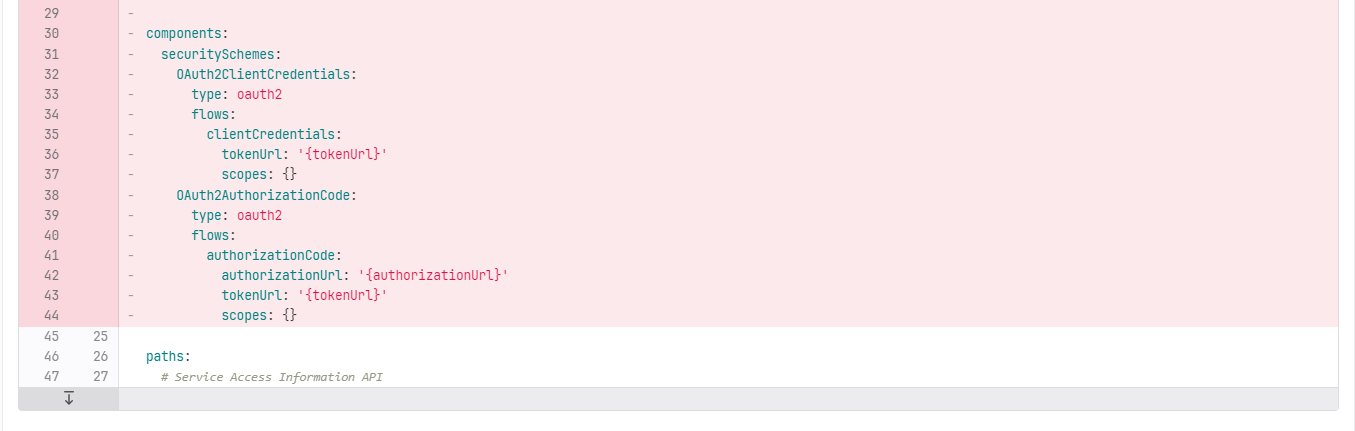












\*\*\*\* Last Change \*\*\*\*