Securitization of calls for US Delete a Look BP x APIM x BP

Context & Problématique

L'APIM sécurise les appels au DCT en validant l'authentification du user.

En prérequis pour que l'APIM puisse faire cette vérification, l'appel à l'APIM doit contenir :
- Le JWT du Client (dans le Header de l'appel)
- Le Gigya ID du client (dans les paramètre de l'appel)

L'APIM compare alors la cohérence entre :
- Le Gigya ID en paramètre
- Le Gigya ID récupéré du JWT

Si les 2 valeurs sont égales, l'appel est transmis au DCT
Sinon, l'appel est refusé

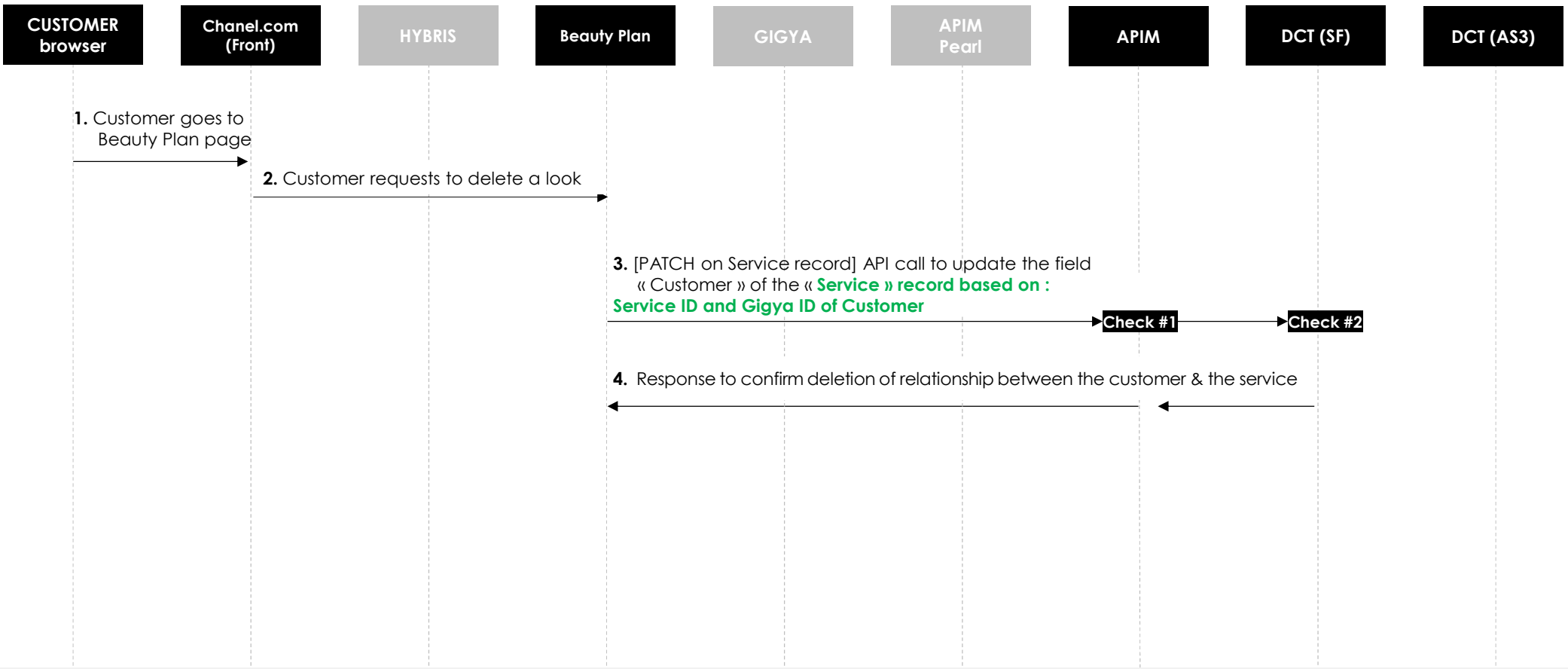
Problématique à adresser : les appels permettant la user story « Delete a look » ne continent pas le Gigya ID en paramètre.
(techniquement c'est un appel de modification au DCT, afin d'anonymiser le lien entre "Customer" et "Service")

Plusieurs solutions ont été proposées pour permettre ce use case : nous avons besoin d'identifier celles qui sont conformes niveau sécurité.

Delete a look **[With APIM]**

DCT data flow details

Caption | **Used in this flow** | **Not used in this flow**



Check #1 (1) SF checks JWT validity and (2) Checks consistency between : Gigya ID in parameter VS Gigya ID in JWT

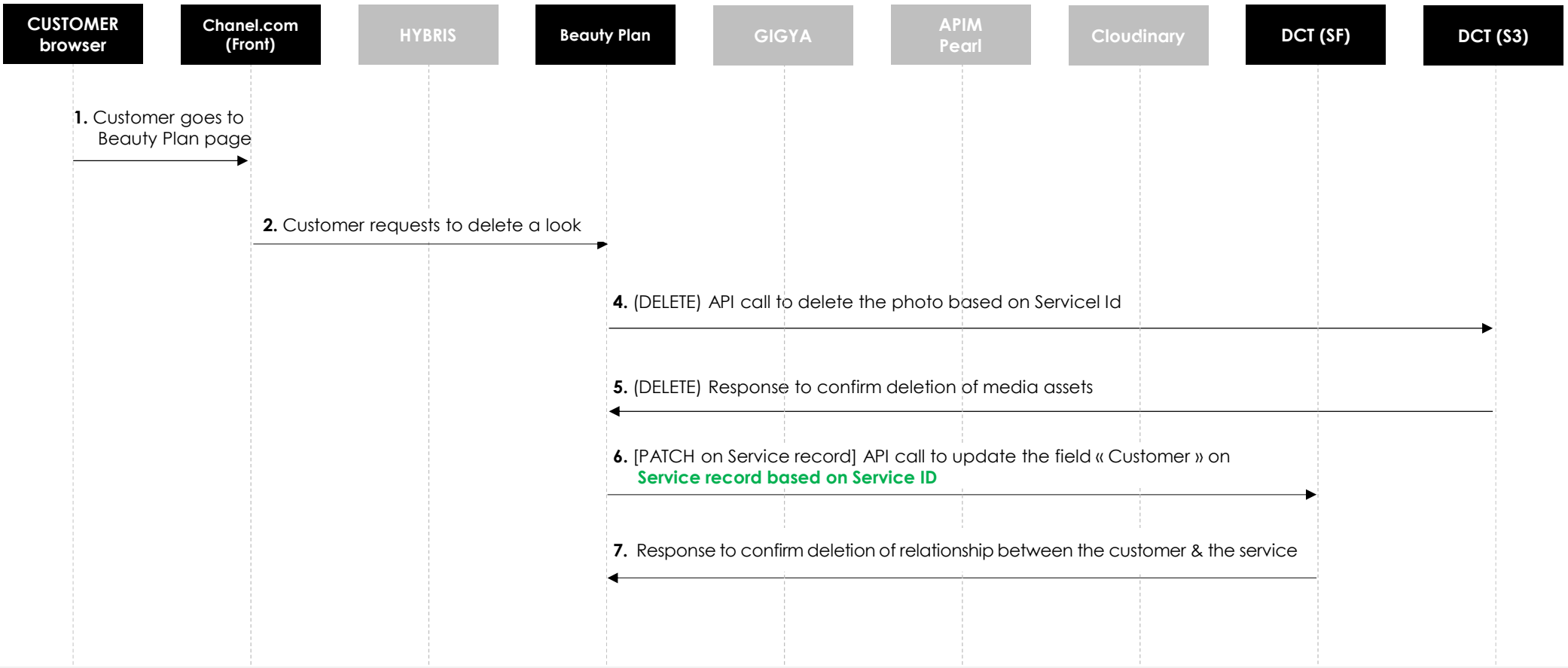
Check #2 SF checks if Gigya ID of the payload is the same as the Gigya ID field of the Customer linked to the Service

Appendices

Delete a look **[OLD - Without APIM]**

DCT data flow details

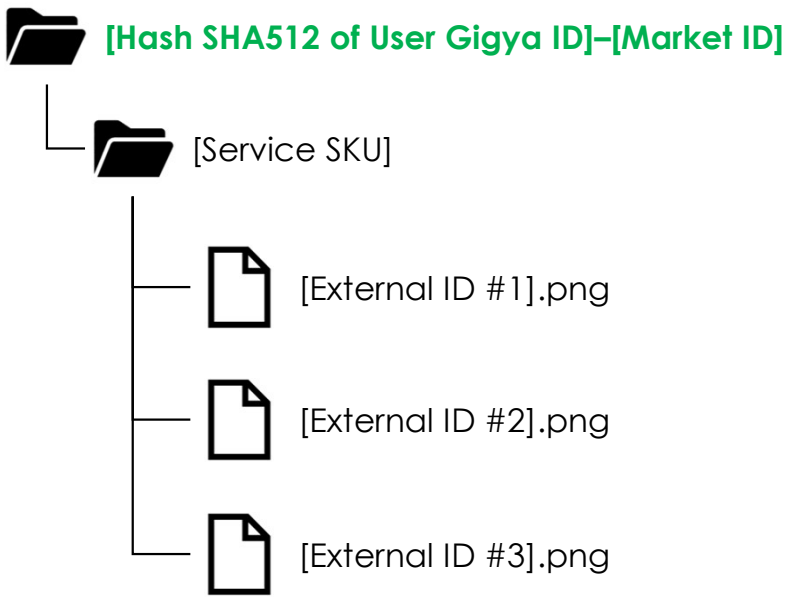
Caption: **Used in this flow** / **Not used in this flow**



- To manage the atomicity of the transaction, we recommend to implement a process to mitigate the risk of having orphaned images in case of error in flow (4), and no error on flow (6)

DCT data models – Folder structure

Amazon S3



Updated on 13/02/2023 to add market information to the name of the client folder
Updated on 13/03/2023 to have SHA512 hash of Gigya ID, instead of Gigya ID in Clear

Salesforce

Customer

Customer Name (Auto Number)
Gigya ID (Text)
Market text)
To be Anonymized

1
*

Service

External ID (Auto Number)
Look (Text)
Market ID (Text)
POS ID (Text)
Service SKU (Number)
Service Name (Auto Number)
Service Number (Number)
Date & Time of the Service (Date)
Date & Time of the Consent (Date)

1
*

Product

Product SKU (Number)
Product Name (Auto Number)
Service External ID (Text)

→ Relation One to Many