Integration Specification: FSVAS

Security Classification:Partner Confidential

Status: Draft

Summary of Revisions:

Version	Date	Author(s)	Comments
0.1	11.11.2014	Mikko Peltonen	Initial Draft
0.2	14.11.2014	Mikko Peltonen	Added Provisioning Flows

1 Introduction

1.1 Purpose of the document

This document defines all integration points that are implemented in the scope of the FSVAS younited delivery project. The document is focused on the Younited project, but the Safe Anywhere family of products are also considered wherever relevant. This is especially the case in the provisioning use cases, since the same provisioning interface (Safe Avenue) is used to provision both products, and FSVAS must take caution to coordinate the API usage across the product families.

Any adaptation(s) to the standard solution is subject to an analysis by a solution architect of F-Secure with support from relevant team(s) of FSVAS. The dedicated solution must be agreed upon between FSVAS and F-Secure.

1.2 Audience

This document is intended for the FSVAS team(s) defining, implementing, testing, validating and operating the provisioning integration with the Safe Avenue environment.

1.3 References

1. safeavenue-int-doc-2.0.1_20131125.pdf. Integration document for Safe Avenue version 2.0.1. F-Secure Corporation, 2013.
2. RFC 6749 The OAuth 2.0 Authorization Framework, Internet Engineering Task Force, 2012.
3. OpenID Connect 1.0 Core. February 26, 2014. OpenID. http://openid.net/specs/openid-connect-core-1_0.html.
4. F-Secure OneID 3.0 - Single Signon With OAuth - Integration Guide.pdf. F-Secure Corporation, 2014.

1.4 Glossary

Customer Account: see Safe Avenue Customer Account.

FSVAS Customer Account: entity in the FSVAS environment that represents an actual customer of FSVAS.

Safe Anywhere: F-Secure's client security product (http://www.f-secure.com/static/doc/operators_global/brochures/safe-anywhere.pdf).

Safe Avenue: F-Secure hosted environment exposing an HTTPS based, REST-like, API. The operations of this API offer a unified account management for the F-Secure security products and the F-Secure younited service.

Safe Avenue Customer Account: entity in the Safe Avenue environment that is holding the access rights to the Safe Anywhere products and to the younited service. This entity corresponds to *one and only one* FSVAS Customer account. The link is established via the external reference attribute which *uniquely* and *persistently* identify the corresponding FSVAS customer account.

User Account: see Safe Avenue User Account.

Safe Avenue User Account: entity in the Safe Avenue environment that holds details about the person making use of the younited service like, for example, username, password, first name and last name.

Younited Grace Period: period starting when the access to the younited service of an account is terminated. All content of the account in the younited service is deleted at the end of the grace period.

Younited Service: F-Secure's multi-tenant Personal Cloud solution.

2 Provisioning Integration

2.1 Safe Avenue API Overview

The Safe Avenue API is the F-Secure provisioning interface giving FSVAS means to manage customer access rights to the F-Secure Safe Anywhere products and to the younited service in a unified manner. Safe Avenue API is an HTTPS based, REST-like interface.

The Safe Avenue environment supports multiple tenants, and each operator is assigned one tenant. In FSVAS case this means that one Safe Avenue tenant with dedicated endpoints will be used for each of the operators (Vivo, Oi and GVT).

The corresponding FSVAS customer account is identified by the external reference attribute of the Safe Avenue customer account. The external reference is a free form string defined by FSVAS and supplied in all requests. It shall uniquely and persistently identify one and only one customer account.

The provisioning use cases defined in this document utilize the following operations that are further explained in the next sections:

- `create_customer`: create a customer account with its initial set of access rights (allocated quota, number of Safe Anywhere licenses) and, possibly, the user account.
- `update_customer`: modify the allocated quota or the number of Safe Anywhere licenses of a given customer account.
- `name_customer`: create the Safe Avenue user account for an existing customer account that doesn't have one yet.
- `suspend_customer`: expire younited account and terminate Safe Anywhere licenses for a given customer account. The consequence of this operation invocation is that the younited subscription will be set to start the grace period (see Appendix B for further details) and all security licenses will be immediately terminated.
- `resume_customer`: resume access to the younited service and re-enable security licenses for a customer account. If invoked during the grace period of a younited account, all customer data is also retained. If invoked after the grace period has ended, will recreate the younited account with the old username and password.

The `echo` operation may be useful to verify access from the FSVAS environments to the Safe Avenue environments:

- echo(): echoes back the supplied message.

2.1.1 Overview of key Safe Avenue Operations

2.1.1.1 Identification and Authentication

The tenant (operator) in Safe Avenue is identified by the request path in the HTTP request. The user is authenticated and authorized by the use of HTTP Basic authentication credentials (Safe Avenue API Credentials). Each set of Safe Avenue API credentials provided by F-Secure will be associated with only a single Safe Avenue tenant.

2.1.1.2 create_customer()

This operation creates a new customer account. The operation takes the allocated quota and the details of the user account for the younited service, and the number of Safe Anywhere licenses as parameters.

The `extref` attribute is a *mandatory* parameter. It defines the external reference of the customer account. It is the only link FSVAS has in the future to the customer account, therefore it is very important that the external references are constructed using an algorithm that guarantees uniqueness and persistency. For example, it is not sufficient to use MSIDN as the external reference, because MSISDN can be transferred to another subscriber during the customer account life span.

The `username` attribute is an *optional* parameter on the API, but it has to be present when SSO is used. It can be populated with the real username that the user shall log in with, but it can alternatively also be a completely opaque identifier, as long as it is guaranteed to be unique in the scope of the operator being provisioned. For example, it can be set to the external reference of the customer.

The `email_addr` attribute is an *optional* parameter on the API, but it has to be present when SSO is used.

The `first_name` attribute is an *optional* parameter on the API, but it has to be present when SSO is used. This attribute is used in the emails that are sent. It is also displayed in the FSVAS Younited client application, but the value can be overwritten upon every login by providing an updated value in the UserInfo response.

The `last_name` attribute is an *optional* parameter on the API, but it has to be present when SSO is used.

The `quota_size` attribute is an *optional* parameter, and it shall be present only when cloud account shall be created upon customer creation. Its value shall be set to the amount of quota to be granted to the user, expressed in megabytes (10^3 bytes). For example, a value of “5000” would grant the user 5 gigabytes or 5,000,000,000 bytes of quota.

The `license_size` attribute is an *optional* parameter with a default value of 0. It shall contain the number of Safe Anywhere licenses available to the customer.

2.1.1.3 update_customer

This operation modifies the number of available Safe Anywhere licenses or the allocated quota.

The `extref` attribute is a *mandatory* parameter. It defines the external reference of the customer account.

The `quota_size` attribute is an *optional* parameter. When supplied, it contains the new allocated quota expressed in megabytes. The amount shall be:

- equal to the trial quota
- or greater than or equal to the maximum app store quota
- or equal to 0. A quota of 0 bytes terminates the younited service for the associated customer account. If the customer account had previously a non zero allocated quota (see Appendix B for further details).

The quota downgrade is already possible in Safe Avenue v2.1 which is currently in production.

The `license_size` attribute is an *optional* parameter. When supplied, it contains the new number of available Safe Anywhere licenses.

2.1.1.4 suspend_customer

This operation suspends all the security licenses and younited subscription for the customer identified by external reference supplied. In the case of younited, the user will still be able to access the data for the duration of the 30 day grace period, after which all data is erased (see Appendix B for further details).

The `extref` attribute is a *mandatory* parameter. It defines the external reference of the customer account to suspend.

2.1.1.5 resume_customer

This operation either resumes the previously suspended security licenses or the younited subscription (when the younited account has been on a grace period). If called on a younited subscriber whose grace period has already passed, the user account will get recreated with the original parameters, but all data previously on the account is erased.

The `extref` attribute is a *mandatory* parameter. It defines the external reference of the customer account to resume.

2.2 Provisioning architecture

2.2.1 External References

External reference is the identifier that FSVAS uses to uniquely refer to the customers created over the Safe Avenue API. External reference is carried in all API requests referring to an individual customer in field `extref`. The choice of external references is an important consideration when designing the Safe Avenue API integration. If the Safe Avenue is used to provision multiple products, the external references shall be selected so that each external reference:

- Identifies one physical customer, not subscription or service
- Is sufficiently unique and persistent, so that the same external reference will always point the same customer

2.3 Use Cases

2.3.1 PUC1a: Activation of new customers (SSO)

2.3.1.1 Description

The creation of a Safe Avenue customer account grants access the Younited and / or SAFE in one operation. This use case is shown in two variations (PUC1a and PUC1b) for SSO and non-SSO flow respectively. While the long term plan is to use SSO for all operators, the non-SSO case is included due to the pending decision on whether the Oi operator will be deployed without SSO first, for expedited launch.

The access to the Younited service requires external reference, a valid quota and identity details to be supplied. The identity details are used to automatically create the user account required to access the younited service.

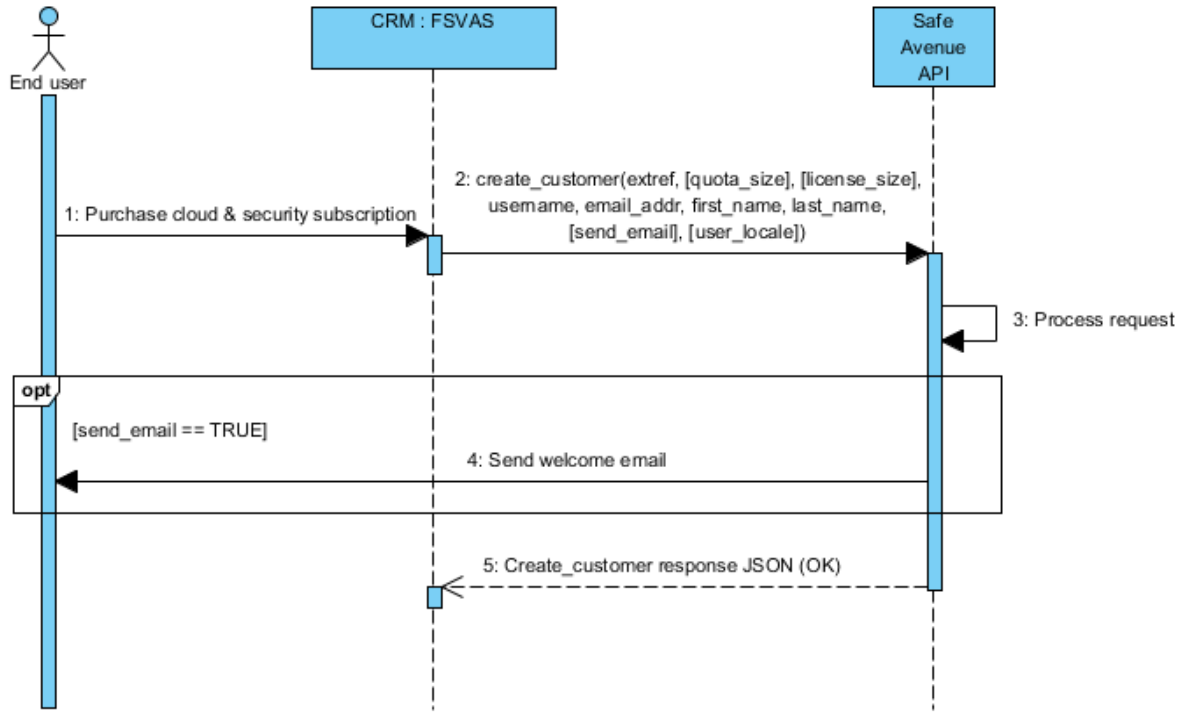
The access to the SAFE service requires external reference, a number of SAFE licenses to be granted, and identity details to be supplied. The identity details are used to automatically create the user account required to access the SAFE service.

In the SSO case, the create_customer call should request Safe Avenue explicitly to not send welcome email, if FSVAS prefers to handle all email communication directly with the end users. FSVAS must supply all details for user creation (username, email_addr, first_name, last_name) in the create_customer() call because the API requires it, but the email address, username and first name supplied may be auto-generated values as long as the values supplied for username and email are always unique.

The operation used for this use case is:

- `create_customer`

2.3.1.2 Sequence Diagram



2.3.1.3 Steps

1. A new FSVAS customer requests access to the younited service.
2. The FSVAS system calls the Safe Avenue `create_customer` operation with the attributes as below:

Parameter name	Value	Presence	Notes
extref	External reference to the customer to be created	Mandatory	
quota_size	Younited quota to be granted in megabytes	Optional	
license_size	Number of SAFE licenses to be granted to the user	Optional	
username	The user name	Required	Must be unique. Should not be set to the real username of the FSVAS IdP user (to permit two external references for the same subscriber). Therefore it must be a fake, unique value such as external reference.
email_addr	The email address to be used as the username	Required	Must be unique and in correct email address format. May be either set to the real email address of the user, or a dummy, unique email address.
first_name	First name of the user to be created	Required	The first name of the user. May be either set to the real first name of the user, or a dummy auto generated value. Note! This value will be visible in some UI elements, unless

			overridden in the UserInfo response
last_name	Last name of the user to be created	Required	The last name of the user. May be either set to the real last name of the user, or a dummy auto generated value.
send_email	0	Optional (default value is 1)	1 if Safe Avenue should send the welcome email, 0 otherwise.
user_locale	The locale of the user	Optional (default value is FSVAS's default locale)	Locales as defined in Safe Avenue manual

3. Safe Avenue processes the request.
4. Safe Avenue responds to the `create_customer` with a successful response.

2.3.2 PUC1b: Activation of new customers (no SSO)

2.3.2.1 Description

This use case is a variation of the PUC1 use case defining the activation flow for operators without SSO.

The access to the Younited service requires external reference, a valid quota and identity details to be supplied. The identity details are used to automatically create the user account required to access the younited service.

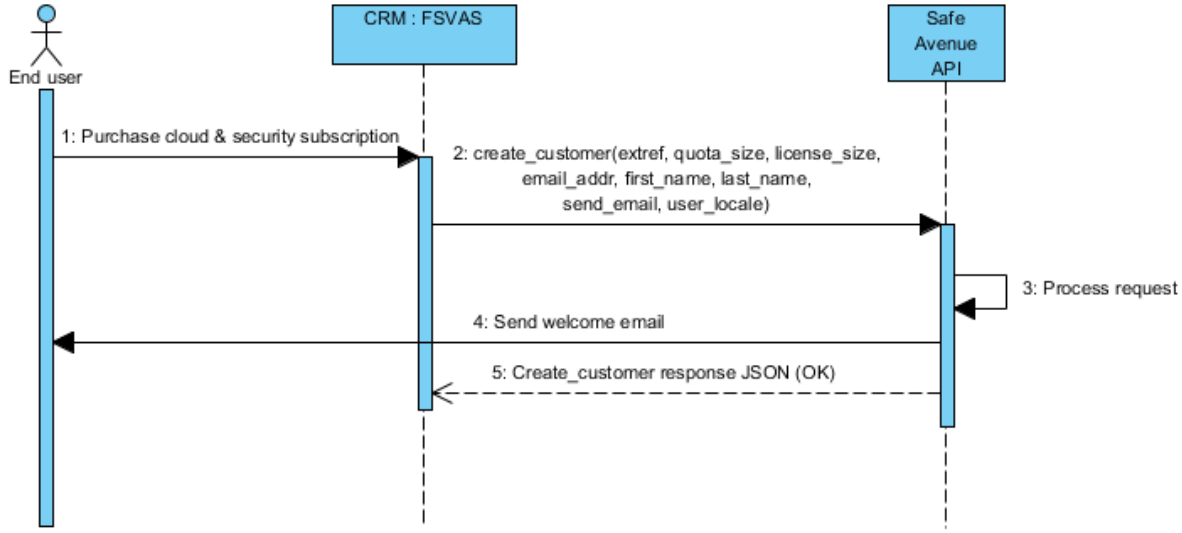
The access to the SAFE service requires external reference, a number of SAFE licenses to be granted, and identity details to be supplied. The identity details are used to automatically create the user account required to access the SAFE service.

In the non-SSO case, Safe Avenue has to send the welcome email with access details (including a generated one-time password) directly to the user. Therefore the key difference of the non-SSO flow is that all of the user details must be actual, and not auto-generated. Also, the username attribute shall not be included in the create_customer() call in this case, because when using F-Secure IdP, the username is always the email address.

The operation used for this use case is:

- `create_customer`

2.3.2.2 Sequence Diagram



2.3.2.3 Steps

5. A new FSVAS customer requests access to the younited service.
6. The FSVAS system calls the Safe Avenue `create_customer` operation with the attributes as below:

Parameter name	Value	Presence	Notes
extref	External reference to the customer to be created	Mandatory	
quota_size	Younited quota to be granted in megabytes	Optional	
license_size	Number of SAFE licenses to be granted to the user	Optional	
email_addr	The email address to be used as the username	Required	Must be unique and in correct email address format, and a real email address that the user has access to. The access details will be sent to this email address.
first_name	First name of the user to be created	Required	The first name of the user. Shall be set to the real first name of the user. The value supplied in this attribute will be visible to the customer in the younited client. User is able to change the value in the Younited client later.
last_name	Last name of the user to be created	Required	The last name of the user. May be either set to the real last name of the user, or a dummy auto generated value. User is able to change

			the value in the Younited client later.
send_email	0	Optional (default value is 1)	1 if Safe Avenue should send the welcome email, 0 otherwise.
user_locale	The locale of the user	Optional (default value is FSVAS's default locale)	Locales as defined in Safe Avenue manual

7. Safe Avenue processes the request.
8. Safe Avenue responds to the `create_customer` with a successful response.

2.3.3 PUC2: Modify Younited quota

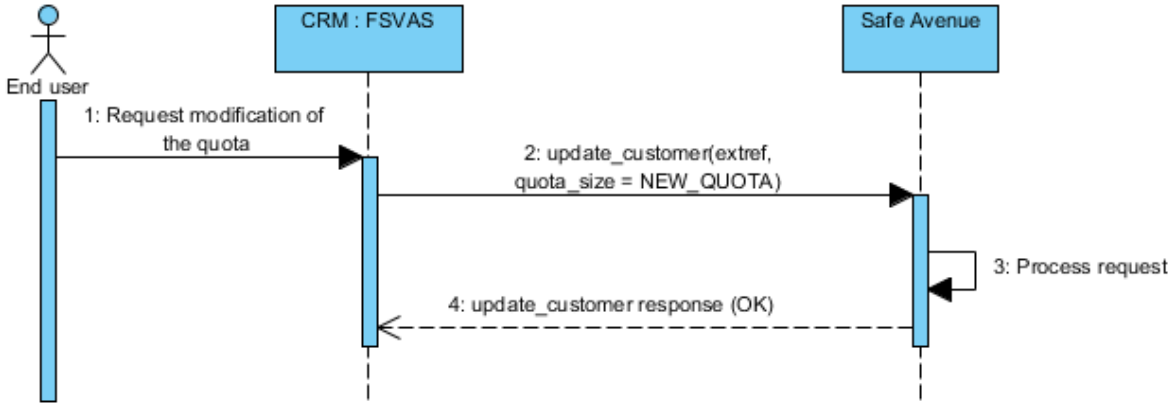
2.3.3.1 Description

Upgrading or downgrading the quota is achieved by updating the customer with a new quota. This operation is called with the same external reference that was used when ordering the initial younited subscription.

The operation used for this use case is:

- `update_customer()`

2.3.3.2 Sequence Diagram



2.3.3.3 Steps

1. An activated FSVAS customer requests upgrade or downgrade of her/his quota to X GB.
2. The FSVAS system requests the quota modification by invoking update_customer() call on the Safe Avenue API. The following attributes are required:

Parameter name	Value	Presence
extref	The external reference to the user whose quota is being altered	Mandatory
quota_size	New quota in megabytes	Optional, must be present to alter the quota

3. Safe Avenue processes the request.
4. Safe Avenue confirms upsizing / downsizing the quota to FSVAS' system in update_customer() response.

2.3.4 PUC3: Terminate Younited subscription retaining SAFE

2.3.4.1 Description

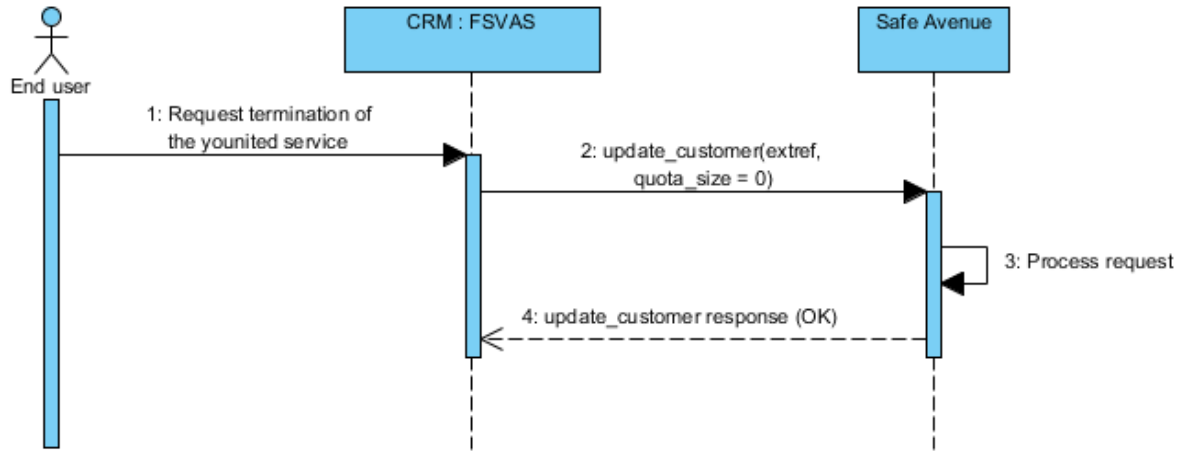
Terminating a Younited external reference is achieved by suspending the external reference in Safe Avenue.

The access to the Younited service will be expired at 00:00 UTC. At that time, the access will enter in the grace period which is automatically reducing the rights granted to the FSVAS customer on the younited service (see Appendix B for further details).

The operation used for this use case is:

- `update_customer`

2.3.4.2 Sequence Diagram



2.3.4.3 Steps

1. An activated FSVAS customer requests to cancel his / her younited service via the FSVAS system.
2. The FSVAS system requests the suspension of the Younited subscription with a call to update_customer(). The following attributes are required:

Parameter name	Value	Presence
extref	External reference of the FSVAS customer account to be suspended	Mandatory
quota_size	0	Optional, setting quota_size to 0 will cause the Younited subscription to be terminated

3. Safe Avenue processes the request.
4. Safe Avenue responds with a successful response to the update_customer() call.

2.3.5 PUC4: Terminate SAFE subscription retaining Younited

2.3.5.1 Description

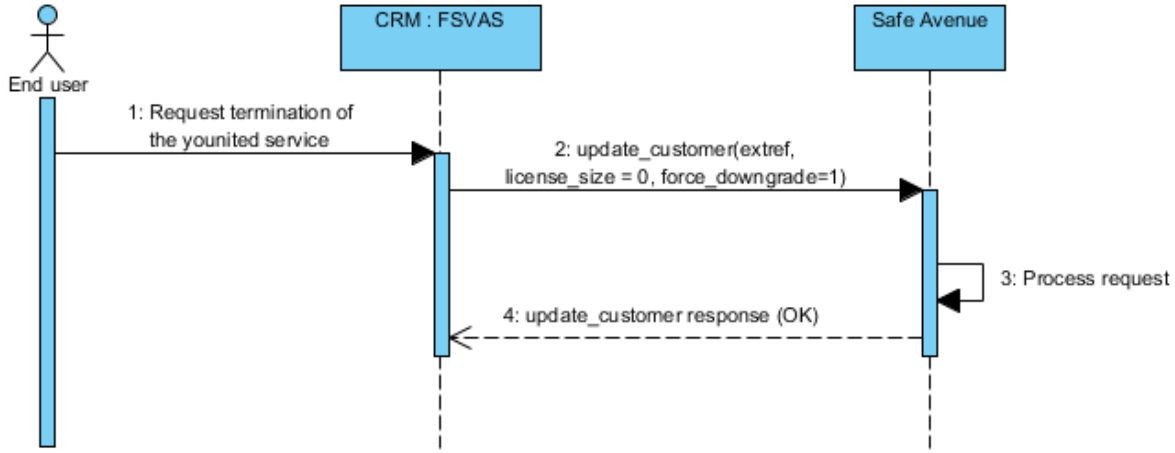
Terminating a SAFE account suspends all the available SAFE licenses.

All the SAFE licenses are immediately suspended preventing the FSVAS customer to use his SAFE clients.

The operation used for this use case is:

- `update_customer`

2.3.5.2 Sequence Diagram



2.3.5.3 Steps

1. An activated FSVAS customer requests to cancel his / her security service via the FSVAS system.
2. The FSVAS system requests the suspension of the customer with a call to update_customer(). The following attributes are required:

Parameter name	Value	Presence
Extref	External reference of the FSVAS customer account to be suspended	Mandatory
License_size	0	Optional, setting license_size to 0 will cause the SAFE subscriptions to be terminated
Force_downgrade	1	Optional; but if user has any used licenses, the operation

		will not terminate the user unless this parameter is present.

3. Safe Avenue processes the request.
4. Safe Avenue responds with a successful response to the update_customer() call.

2.3.6 PUC5: Suspending / terminating a customer

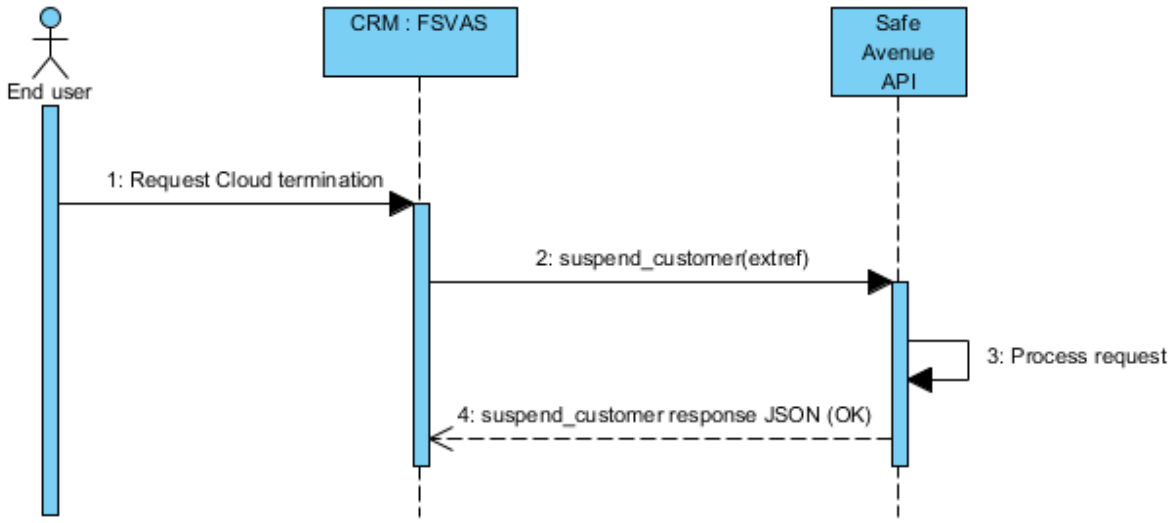
2.3.6.1 Description

This use case illustrates the use of the `suspend_customer` operation that can be invoked to temporarily suspend a customer who is currently on the Younited grace period or has the SAFE licenses disabled.

On Younited this operation will start the grace period of 30 days, during which the user can only access the service using desktop & web clients to read or delete contents from the account.After the grace period is completed, the user's account will be deleted.

On SAFE this operation will disable all SAFE licenses, preventing the FSVAS customer to use his SAFE clients.

2.3.6.2 Sequence Diagram



2.3.6.3 Steps

1. A FSVAS system invokes the Safe Avenue API operation suspend_customer() with following attributes:

Parameter name	Value	Presence	Notes
Extref	External reference of the FSVAS customer account to be suspended	Mandatory	All services of the external reference will be terminated

2. Safe Avenue processes the request.
3. Safe Avenue responds to the suspend_customer() operation with a successful response.

2.3.7 PUC6: Reactivating younited and cloud subscriptions after suspension

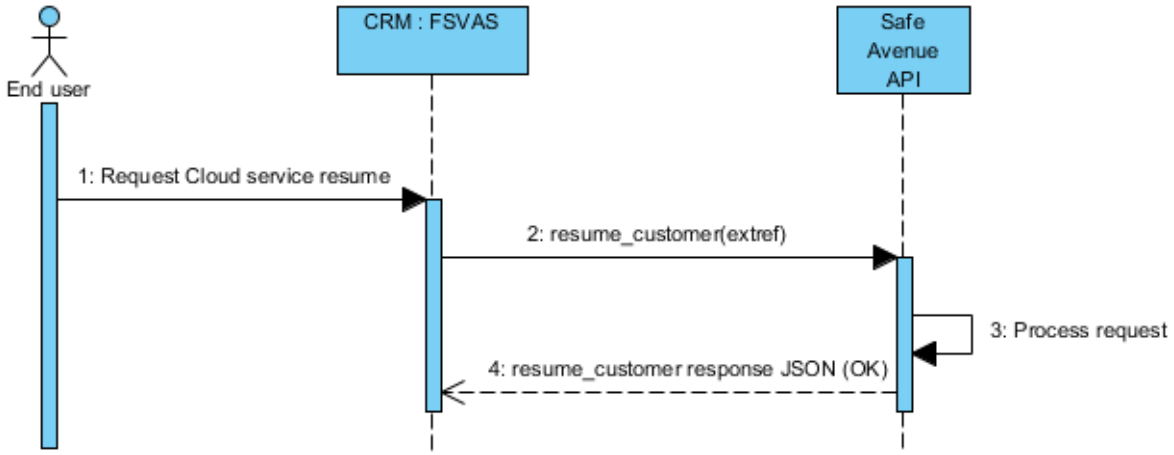
2.3.7.1 Description

This use case illustrates the use of the `resume_customer` operation that can be invoked on a customer who is currently on the Younited grace period or has the SAFE licenses disabled.

On Younited this operation will end the grace period, and set the user's younited subscription back to active state.

On SAFE this operation will enable all SAFE subscriptions which were disabled with suspend_customer operation.

2.3.7.2 Sequence Diagram



2.3.7.3 Steps

4. A FSVAS customer requests to reactivate the Younited or SAFE account that was previously set to grace period (through the use of suspend_customer() as defined above.
5. A FSVAS system invokes the Safe Avenue API operation resume_customer() with following attributes:

Parameter name	Value	Presence	Notes
Extref	External reference of the FSVAS customer account to be resumed	Mandatory	All services of the external reference will be resumed

6. Safe Avenue processes the request.
7. Safe Avenue responds to the resume_customer() operation with a successful response.

3 Authentication Integration

3.1 Authentication Architecture

The F-Secure products based on username / password based licensing will integrate to FSVAS's IdP for authentication. The single sign-on shall be based on OAuth2 protocol as defined in [2], and F-Secure standard implementation of OAuth2-based SSO is defined in [4]. The users will log in to F-Secure services using their FSVAS portal credentials. This is achieved by F-Secure's authentication backend, OneID, federating the authentication to the FSVAS IdP.

The FSVAS user account is usable for all F-Secure products that are based on username / password based licensing. At the moment, the products using username / password are:

- Younited (Younited)
- SAFE (Android)
- SAFE (iOS)
- SAFE (Windows Phone 8)

In the future, all SAFE products will be using username / password based authentication.

Use of SSO has some key implications to the solution. Certain restrictions traditionally enforced by F-Secure's IdP do not hold. For example, user names do not need to be in email address format when using SSO. Also, it shifts some responsibilities from F-Secure to FSVAS. It is FSVAS's responsibility to implement all login / logout pages, and ensure that they are displayed properly on all supported clients. Also password and user profile changes shall all be handled on the FSVAS side.

3.1.1 External Reference Assignment

FSVAS shall assign external references so that for a single user, all services are provisioned under one external reference only. External references must always be unique within a single operator. External references do not strictly have to be unique across operators, but it is recommended.

3.1.2 Authentication Endpoints

3.1.2.1 Authorization Query

F-Secure's younited clients will issue an HTTP GET request to the FSVAS's IdP. The request uses HTTP Basic authentication with client_id:client_secret pair supplied by FSVAS as authorization. The successful authorization response from FSVAS's IdP shall contain the authorization code which is later used by F-Secure OneID to retrieve the access token.

Scope of the authorization requests issued as part of user login flow should include values "profile" and "openid".

The following table defines the parameters F-Secure OneID sets in the request.

Parameter	Description	Presence
response_type	Authorization type requested. Value shall always be set to 'code'	Mandatory
client_id	client_id as supplied by FSVAS for the service in question	Mandatory
scope	Scope of authorization requested. Access token may be restricted using scope	Optional in OAuth, in this integration always set to "openid", "profile"
state	Any opaque value that is carried over across all OAuth requests of a transaction to prevent cross-site request forgery	Optional. If present, must be returned back in the callback query with the same value.
redirect_uri	The URI where the FSVAS IdP should redirect the browser after the successful authentication	Optional in RFC; always set by OneID

3.1.2.2 Token Query

F-Secure OneID will issue an HTTP POST request to exchange the authorization code to a FSVAS's IdP. The request uses HTTP Basic authentication with client_id:client_secret pair supplied by FSVAS as authorization.

Parameter	Description	Presence
code	Authorization code returned by the authorization endpoint	Mandatory
grant_type	Authorization_code	Mandatory
redirect_uri	The URI where the FSVAS IdP should redirect the browser after the successful authentication	Always set by OneID to value identical to the one used in authorization query
client_id	The client ID supplied by FSVAS	Always present
client_secret	The client secret supplied by FSVAS	Always present

The token query response must be a valid JSON object, as defined in section 4.1.2 of RFC 6749.

The token endpoint may include id_token attribute in the token response. However, this is optional, and the value will be ignored by F-Secure OneID. F-Secure OneID requires all user data to be returned in the User Profile query (see next section).

3.1.3 User Profile Query Endpoint

F-Secure OneID shall make the User Profile query using UserInfo endpoint as defined in OpenID Connect Core specification, section 5.3.

The request shall use HTTP GET method. The access token as received from the token endpoint shall be used as the authorization. The access token serves as the sole identification of the user at the user profile query stage, since that is all F-Secure OneID knows about the user at this stage.

3.1.3.1 Supported OpenID Claims

F-Secure OneID can support the OpenID Connect claims as defined in the table below.

Claim	Description	Presence
sub	External reference of the FSVAS customer account	Mandatory
given_name	User's given name	Mandatory. The value shall be displayed on the first and second rows of the "Hi <given_name>" menu of the younited desktop and web clients.
family_name	User's family name	Optional
email	User's email address	Optional
locale	User's locale represented as a BCP47 [RFC5646] language tag	Optional (Default value FSVAS's default locale, nl_NL)
preferred_username	User's username that can be displayed on the client	Optional. Currently not supported by younited clients.
display_name	User's username that can be displayed on the client	Optional. If present,will be displayed on the third row of the "Hi <given_name>"

		menu of the younited desktop and Web clients.

Distributed and Aggregated claims (see OpenID Connect Core specification, section 5.6) shall not be supported by this integration.

3.1.4 Logout

Implemented logout scenarios are application initiated logout and IdP-initiated logoff. Both of the log off flows will be implemented using browser redirects as defined in [4].

3.1.4.1 Administrative logout

OneID does not currently support administrative revocation of the user tokens. However, this might be possible in the future via a direct backend call to OneID.

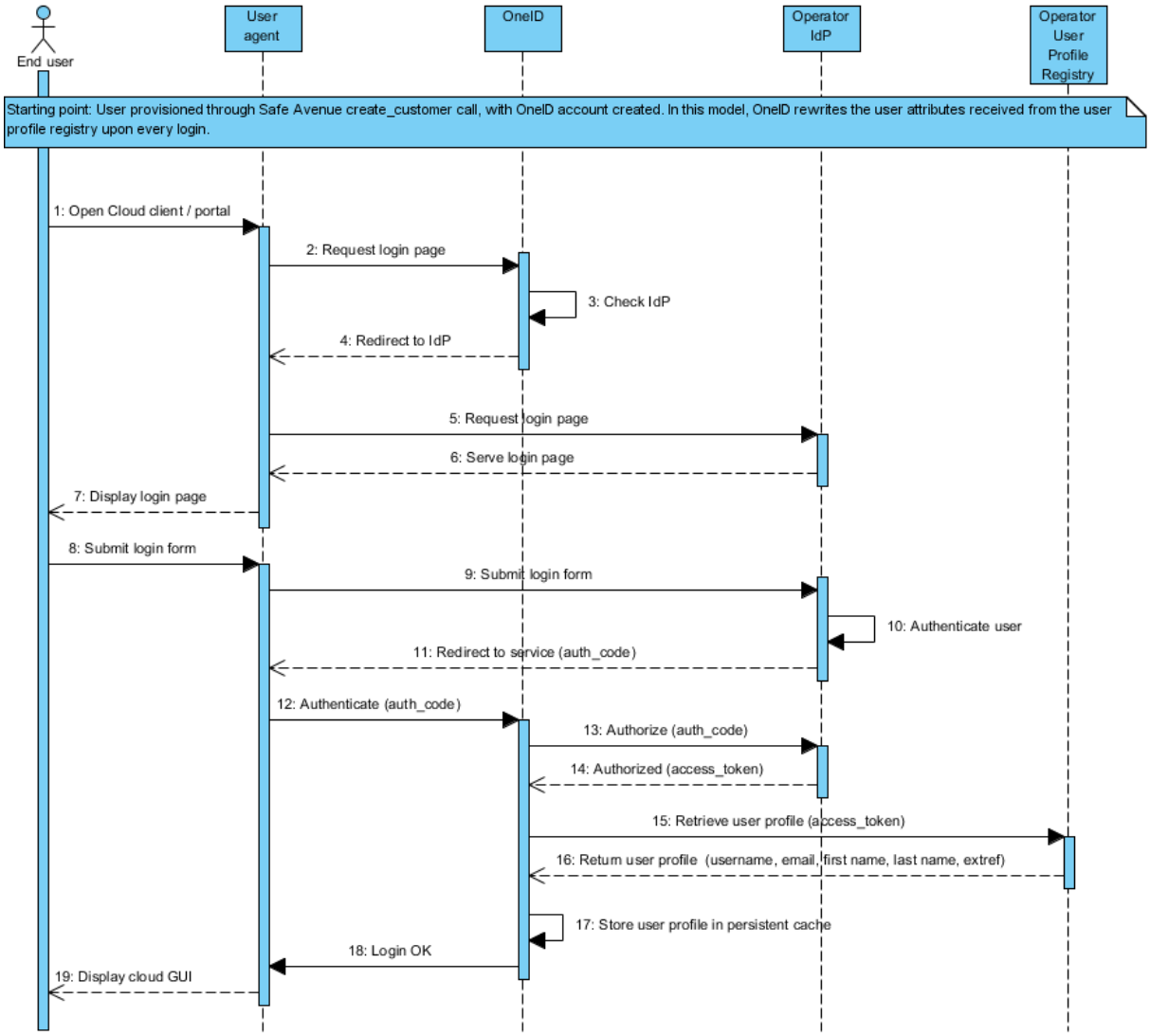
3.2 Authentication Use Cases

3.2.1 AUC1: Login to younited for FSVAS customers

3.2.1.1 Description

The starting point for this use case is that the user has been provisioned using the Safe Avenue API (see 2.3.1 and 2.3.2 for details), and younited client is installed on the customer's device.

3.2.1.2 Sequence Diagram



3.2.1.3 Steps

1. End user opens a Younited client.
2. The client doesn't have a valid authorization token stored, so requests the younited login screen from OneID. The client passes the operator ID of the branded client to OneID.:
3. OneID resolves the IdP to be used for the given operator ID.
4. OneID redirects the client to the FSVAS IdP Authorize endpoint.
5. The client follows the redirect to FSVAS IdP Authorize endpoint.
6. FSVAS IdP responds with a login page.
7. User agent displays the login page to the user.

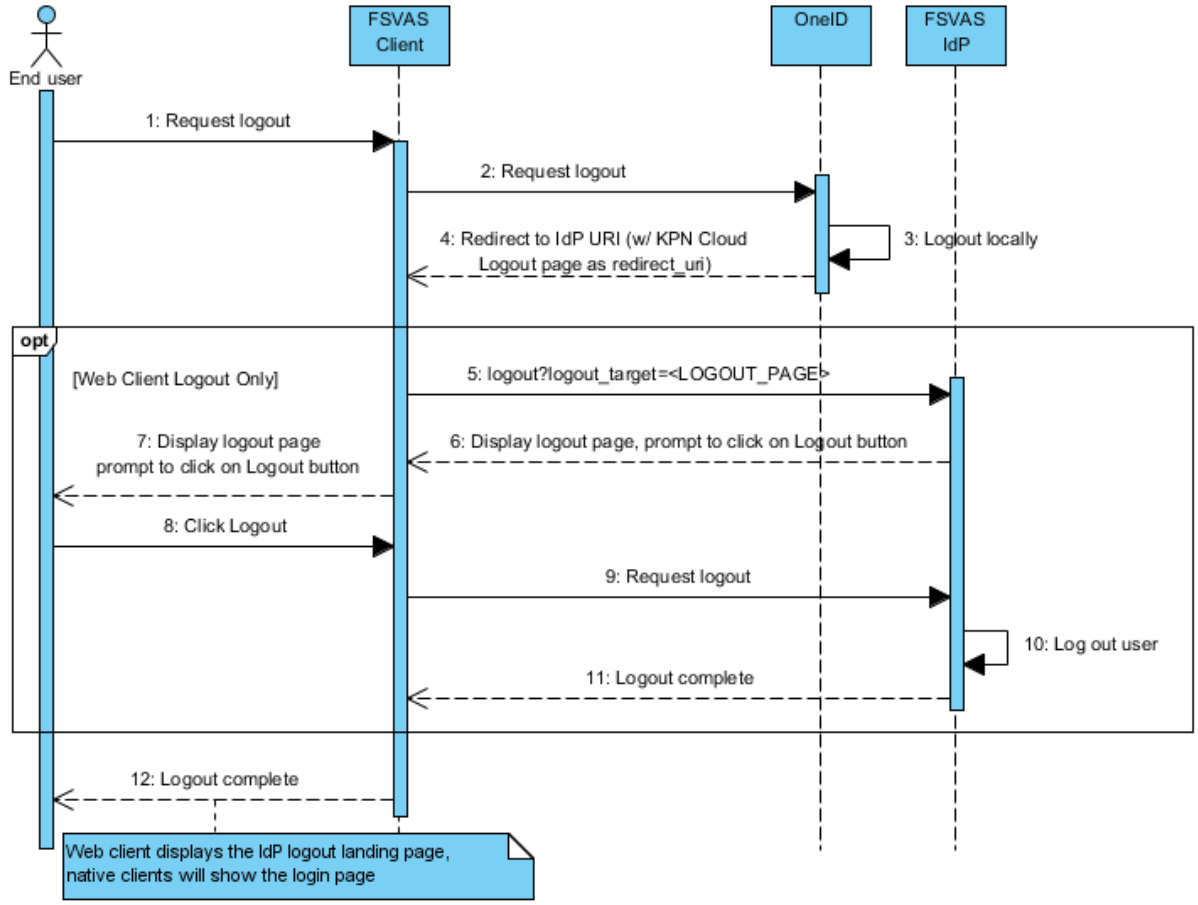
8. User submits the login form.
9. Browser sends the HTTP request to FSVAS IdP to log in.
10. FSVAS IdP authenticates the user.
11. FSVAS IdP responds to the login HTTP request by sending back a HTTP 3xx redirect to the OneID URL with the authorization code and state parameters as in the original request.
12. The browser follows the redirect.
13. OneID requests validation for the authorization code from FSVAS IdP.
14. FSVAS IdP verifies the authorization code and returns an access token (in bearer token format) to OneID.
15. OneID makes the user profile query to userinfo endpoint from FSVAS IdP (User Profile Registry) using OpenID Connect. This step is performed on every login.
16. FSVAS IdP (User Profile Registry) responds with the user profile.
17. OneID stores the user profile in the persistent cache.
18. OneID responds to the client that the login was successful by including an access token and refresh token in the response. The client can now proceed to use the F-Secure services with the access token granted.

3.2.2 AUC2: Logout from client

3.2.2.1 Description

The starting point for this use case is that the user has logged into FSVAS younited client.

3.2.2.2 Sequence Diagram



3.2.2.3 Steps

1. User is currently logged in, and clicks on a Logout link in a FSVAS younited client.
2. User agent requests logout from OneID.
3. OneID logs out the user locally.
4. OneID responds to the HTTP request with a HTTP redirect to FSVAS IdP to log out the user.
5. [Web client only] User agent follows the HTTP redirect to FSVAS IdP logout endpoint.
6. [Web client only] FSVAS IdP returns a logout page, prompting the user to click on the Logout button.
7. [Web client only] The client displays the logout page to the user.
8. [Web client only] The user clicks on the Logout button.

9. [Web client only] The client makes a HTTP request to FSVAS IdP logout endpoint.
10. [Web client only] FSVAS IdP logs out the user.
11. [Web client only] FSVAS IdP returns the logout complete page.
12. The client displays the logout landing page to the user. For the web client users, the landing page will be a logout page saying that the user has been logged out. For native clients supporting logout, the user will be displayed the login page.

Appendix A. Safe Avenue API Usage Guidelines

A.1. Synchronicity and real time operation

All Safe Avenue client applications must take into consideration two very important properties of the Safe Avenue operations. The first property is synchronicity. It implies that Safe Avenue client applications must wait for responses. The second property is the non real-time processing. This property implies that Safe Avenue client applications must not wait forever for responses. A typical Safe Avenue client application adapts to these two properties by blocking its execution flow for only a fixed period of time (i.e. timeout).

The recommended timeout is 10 minutes which is the timeout value of Safe Avenue. That high value allows for rare, but possible, situations where the Safe Avenue system is highly loaded.

Even if the recommended timeout is 10 minutes, the Safe Avenue operations are quite fast in general. Customer creation, customer update and user account operations typically return within a couple of seconds.

Attention must be paid to use cases where a user interface utilizes Safe Avenue operations. The user interface shouldn't directly call the Safe Avenue operations since it could degrade its responsiveness.

A.2. Error Handling

A.2.1. Strategies according to kind of error

Safe Avenue API defines generic error codes to report error conditions that are common for most operations. These generic error codes are documented in the Safe Avenue Integration document under section 6.5, Resource Errors. Error codes pertinent to the operation being called are documented in the Safe Avenue Integration document under each operation. Both kinds of errors must be caught by the Safe Avenue client applications.

According to the kind of error, different strategies should be adopted:

- **Technical errors:** these errors are, for example, timeout, connection lost, connection reset by peer or server error HTTP status 500. For this kind of errors, the Safe Avenue operation call should be reissued up to a limited number of times like, for example, 3. It is only when this limit is reached that the Safe Avenue operation should be considered as failed and handled as such.
- **Functional errors:** these errors are, for example, missing or malformed data in mandatory fields, wrong patterns or authentication errors. They are typically related to the Safe Avenue client implementation or configuration and should occur at development time or at deployment time. These errors must not happen in production. If such an error occurs in production, it must be immediately escalated.
- **Business errors:** these errors are, for example, customer not found or external reference does not exist. These kinds of errors shall be handled using the most appropriate way in each case.

A.2.2. Fail Safe!

As with any programming interface, the Safe Avenue API operations can sometime fail, due to various reasons. There can be a scheduled maintenance break (never without advance partner notification), connectivity issues between FSVAS backends and F-Secure ones, incidents in the backends Safe Avenue uses, invalid attribute values, failed authentication, … Thus it is very important to implement the provisioning processes and the Safe Avenue API clients in a fail safe manner, meaning being prepared for error situations.

A.2.3. Make everything possible configurable

It is always a good idea to implement the provisioning process and the Safe Avenue client applications in such manner that changing the business rules or parameters is as unintrusive as possible. For example, changing the Safe Avenue authentication credentials should not necessarily require stopping, modifying and re-testing the in-production provisioning process.

Appendix B. Younited User Experience Modes

The following table defines availability of the main features of the Younited service according to the account status.

Status	Login	Browse	Up load	Down load	Stream	Delete	Create Share	Access Shares	Content
Enabled	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Stored
Over-quota	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Stored
Ceased-GP	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Stored
Ceased Done[1]	No	No	No	No	No	No	No	No	Deleted

The status are based on subscription modifications:

- *Enabled*: the younited subscription is valid.
- *Over-quota*: the user downsized his quota to a level below his current usage in FSIO.
- *Ceased-GP*: the younited subscription has been expired. That starts the Grace Period. The duration of this period is a platform-wide configuration, i.e. all tenants share the same configuration.
- *Ceased Done*: the grace period has finished. The storage content and the storage account are deleted from the Content Cloud platform. The customer created via Safe Avenue API remains present on the Content Cloud platform. The Ceased Done status is not an actual status. Its main purpose is to clarify features availability with respect to the subscription lifecycle.

[1]Ceased Done is not an actual status. It refers to a virtual period of time that starts at the end of the Ceased grace period and that never ends.