

SPEC-ESH

| | |
|---------------|---------------------|
| Last changed: | 20.11.2025 10:20:30 |
| Version: | 3.0.0-rc.6 |
| Creator: | VDV ETS |

Table of Contents

| | | |
|-------|--|----|
| 1 | Scheme Manager | 4 |
| 1.1 | Hotlist Service | 5 |
| 1.1.1 | Hotlist Service System | 6 |
| 1.2 | Media Public Key Infrastructure | 6 |
| 1.2.1 | Certificate retrieval service | 7 |
| 1.3 | Scheme Manager System | 7 |
| 1.4 | (((eTicket Security Hub | 7 |
| 1.4.1 | Certificate Interface | 7 |
| 1.4.2 | Media Configuration Interface | 7 |
| 1.4.3 | Application Owner Module | 7 |
| 1.4.4 | Registrar Module | 7 |
| 1.4.5 | Security Manager Module | 7 |
| 1.5 | Media Management System | 7 |
| 1.5.1 | MediaManagementSystemPort | 8 |
| 2 | ESH Security Management | 8 |
| 2.1 | Overview | 8 |
| 2.2 | Use Cases | 8 |
| 2.2.1 | Handle authentication key hotlisting demand | 8 |
| 2.2.2 | Handle revocation for authentication key hotlisting demand | 11 |
| 2.2.3 | Check and add SAM to hotlist | 13 |
| 2.2.4 | Handle revocation for SAM hotlisting demand | 15 |
| 2.2.5 | Handle request to determine SAM owner | 17 |
| 2.2.6 | Get unclaimed list information | 19 |
| 2.2.7 | Update authentication key hotlist inventory | 21 |
| 2.2.8 | Update SAM hotlist inventory | 23 |
| 3 | ESH Application Owner | 25 |
| 3.1 | Overview | 25 |
| 3.2 | Use Cases | 25 |
| 3.2.1 | Handle request to determine UM app instance ID for Medium ID | 25 |
| 3.2.2 | Terminate UM application | 28 |
| 4 | ESH Registrar | 30 |
| 4.1 | Overview | 30 |
| 4.2 | Use Cases | 30 |
| 4.2.1 | Handle organisation hotlisting demand | 30 |
| 4.2.2 | Handle revocation for organisation hotlisting demand | 32 |
| 4.2.3 | Update organisation hotlist inventory | 34 |
| 4.2.4 | Process retrieval request for organisation list | 36 |

1 Scheme Manager

This chapter contains all components and interfaces concerning the [Scheme Manager](#).

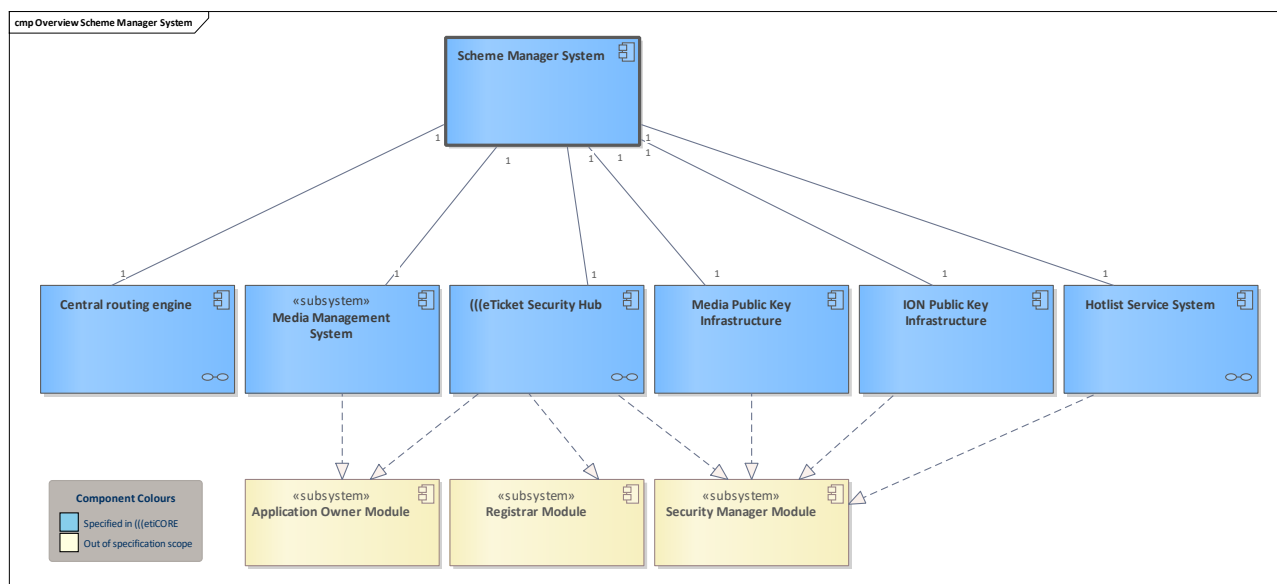


Figure 1: Overview Scheme Manager System

Shows the composition of a [Scheme Manager System](#).

For ION messaging components, see [System Components and Interfaces : Overview of ION components and interfaces](#).

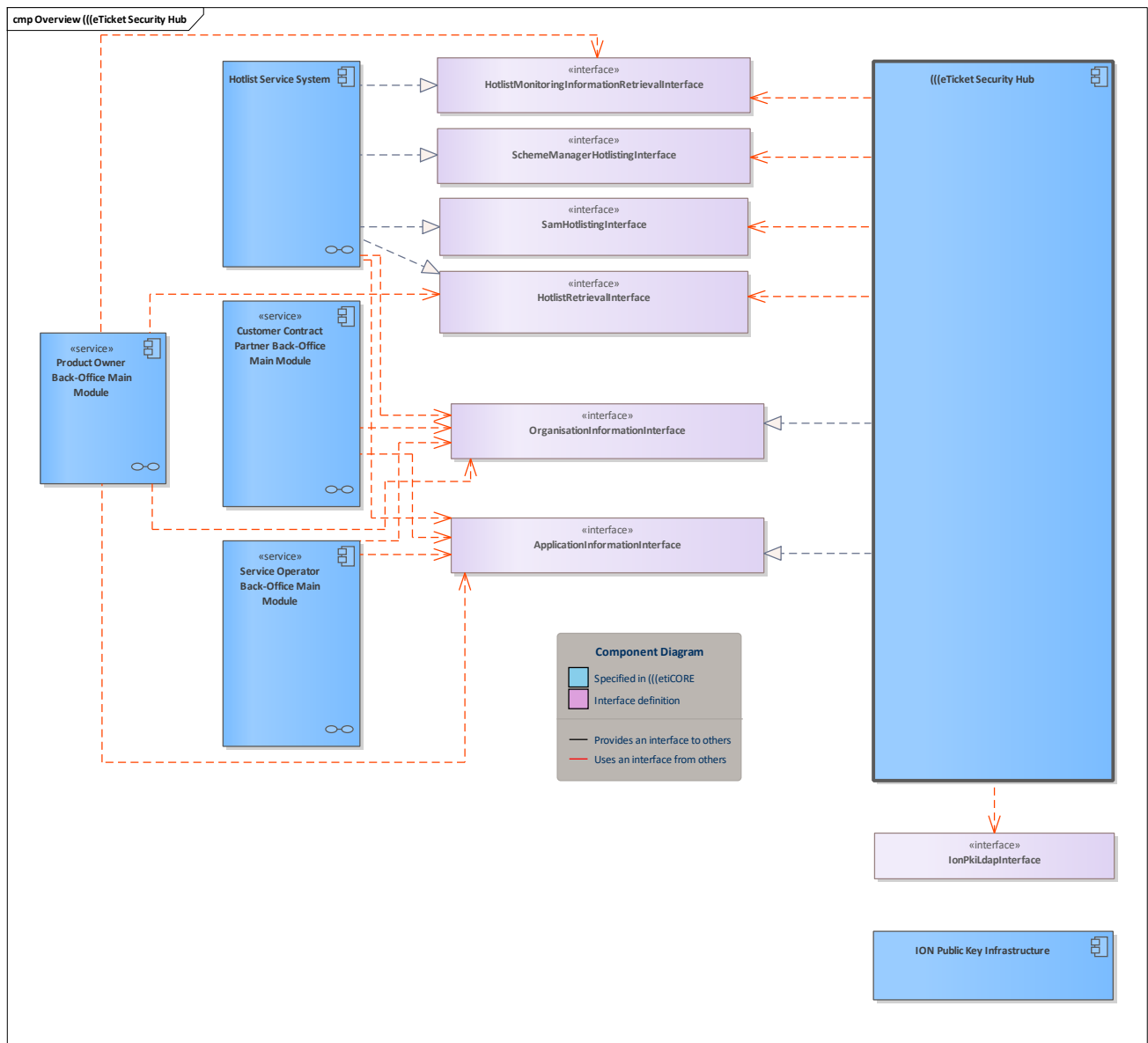


Figure 2: Overview (((eTicket Security Hub

Shows the interaction of the [\(\(\(eTicket Security Hub](#) via interfaces with other components.

1.1 Hotlist Service

This chapter contains all components and interfaces concerning the [Hotlist Service](#) as part of the [Scheme Manager](#).

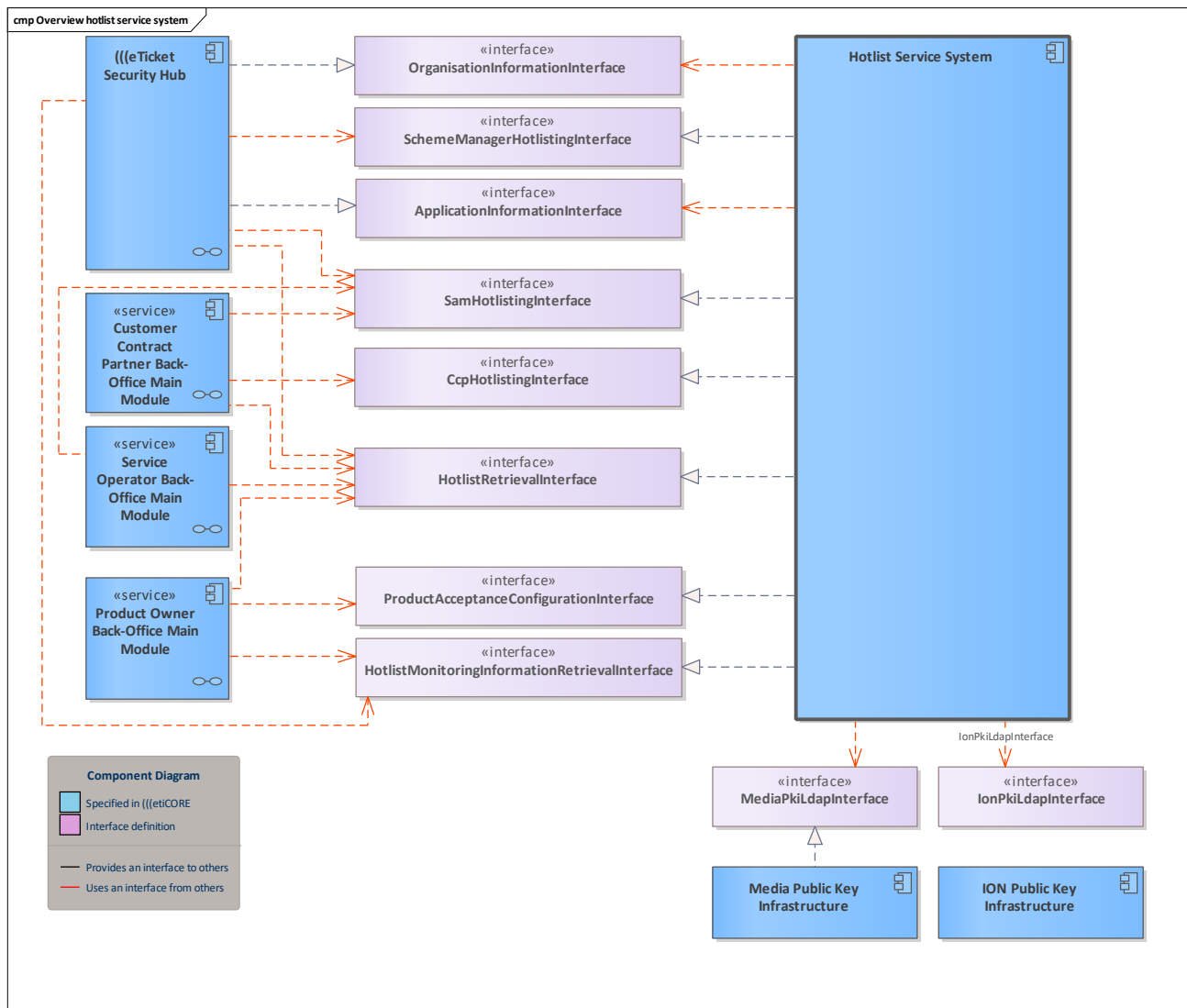


Figure 3: Overview hotlist service system

This diagram shows the interfaces which are implemented and used by the hotlist service system.

1.1.1 Hotlist Service System

System (component) which implements the necessary functionality for the [Hotlist Service](#) and implements interfaces for

- the [Application Owner Module](#),
- [Security Manager Module](#),
- [Customer Contract Partner System](#),
- [Service Operator System](#) and
- [Product Owner System](#).

1.2 Media Public Key Infrastructure

Component for the PKI of the media. The certificates of the user media and SAMs are stored in this PKI.



1.2.1 Certificate retrieval service

Interface that provides the possibility to get a certain certificate of a user medium.

1.3 Scheme Manager System

Component for the [Scheme Manager](#) which implements the related system.

The scheme manager system consists of separate subsystems

- [Hotlist Service System](#)
- [Media Management System](#)
- [\(\(\(eTicket Security Hub](#)
- [Media Public Key Infrastructure](#)
- The ION messaging components such as the [Central routing engine](#) and [ION Public Key Infrastructure](#) (not shown in the overview diagram)

1.4 (((eTicket Security Hub

System (component) which implements the necessary functionality for the [Scheme Manager](#) and consists of

- the [Application Owner Module](#),
- [Registrar Module](#) and
- [Security Manager Module](#)

1.4.1 Certificate Interface

Interface to obtain the CA certificates and the revocation list for CV certificates.

1.4.2 Media Configuration Interface

Interface for card manufacturers and mass personalisers to configure a set of user media or a single user medium. The response contains 1..* configuration scripts which have to be applied to the user media.

1.4.3 Application Owner Module

Component which implements the necessary functionality for the [Application Owner](#).

1.4.4 Registrar Module

Component which implements the necessary functionality for the [Registrar](#).

1.4.5 Security Manager Module

Component which implements the necessary functionality for the [Security Manager](#).

1.5 Media Management System

Component for the media management for user media and SAMs.



1.5.1 MediaManagementSystemPort

Interface that provides operations for the [Media Management System](#).

2 ESH Security Management

Functionality bundle that covers the use cases of the scheme manager's security management.

2.1 Overview

[Handle authentication key hotlisting demand](#)

[Handle revocation for authentication key hotlisting demand](#)

[Check and add SAM to hotlist](#)

[Handle revocation for SAM hotlisting demand](#)

[Handle request to determine SAM owner](#)

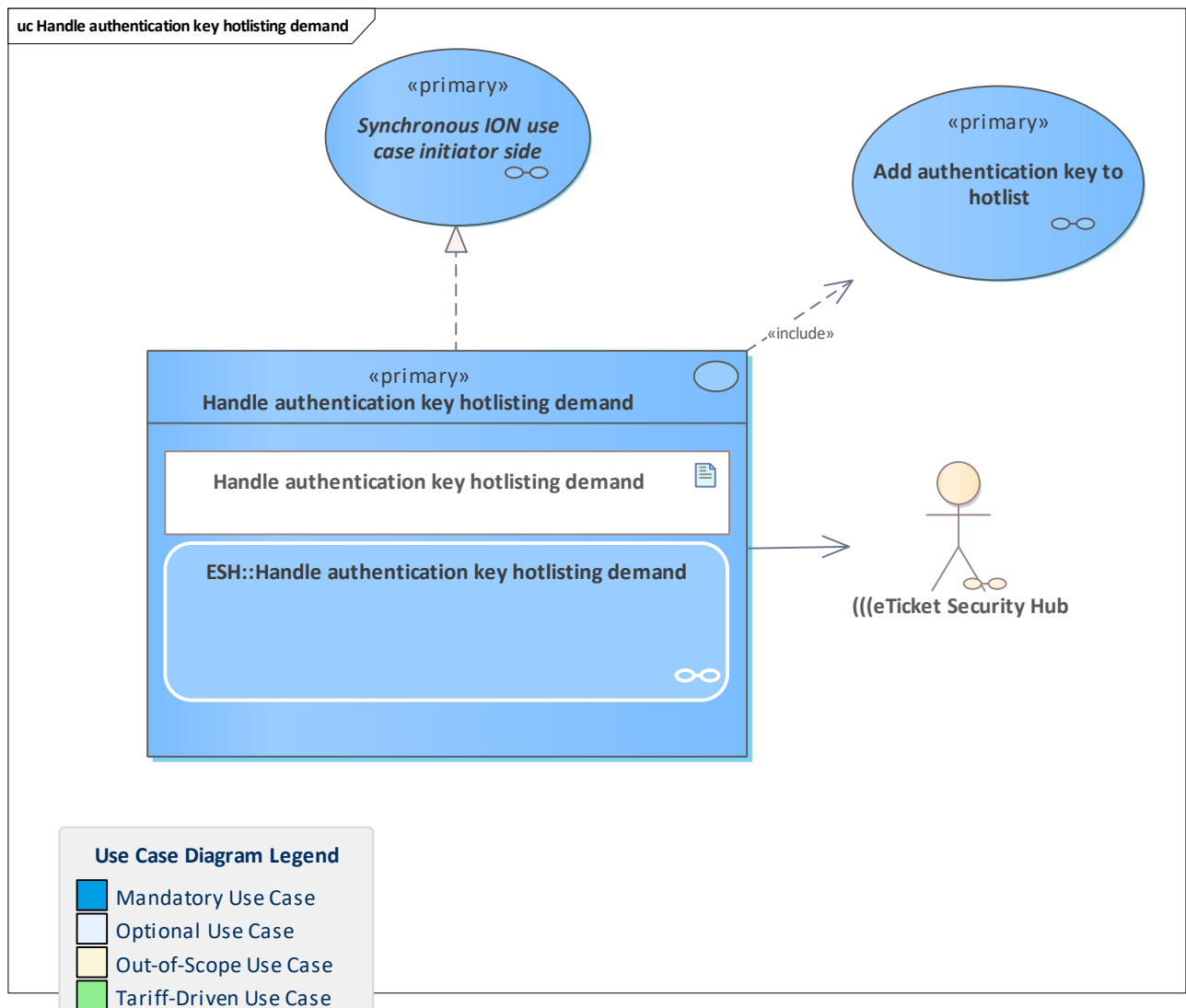
[Get unclaimed list information](#)

[Update authentication key hotlist inventory](#)

[Update SAM hotlist inventory](#)

2.2 Use Cases

2.2.1 Handle authentication key hotlisting demand

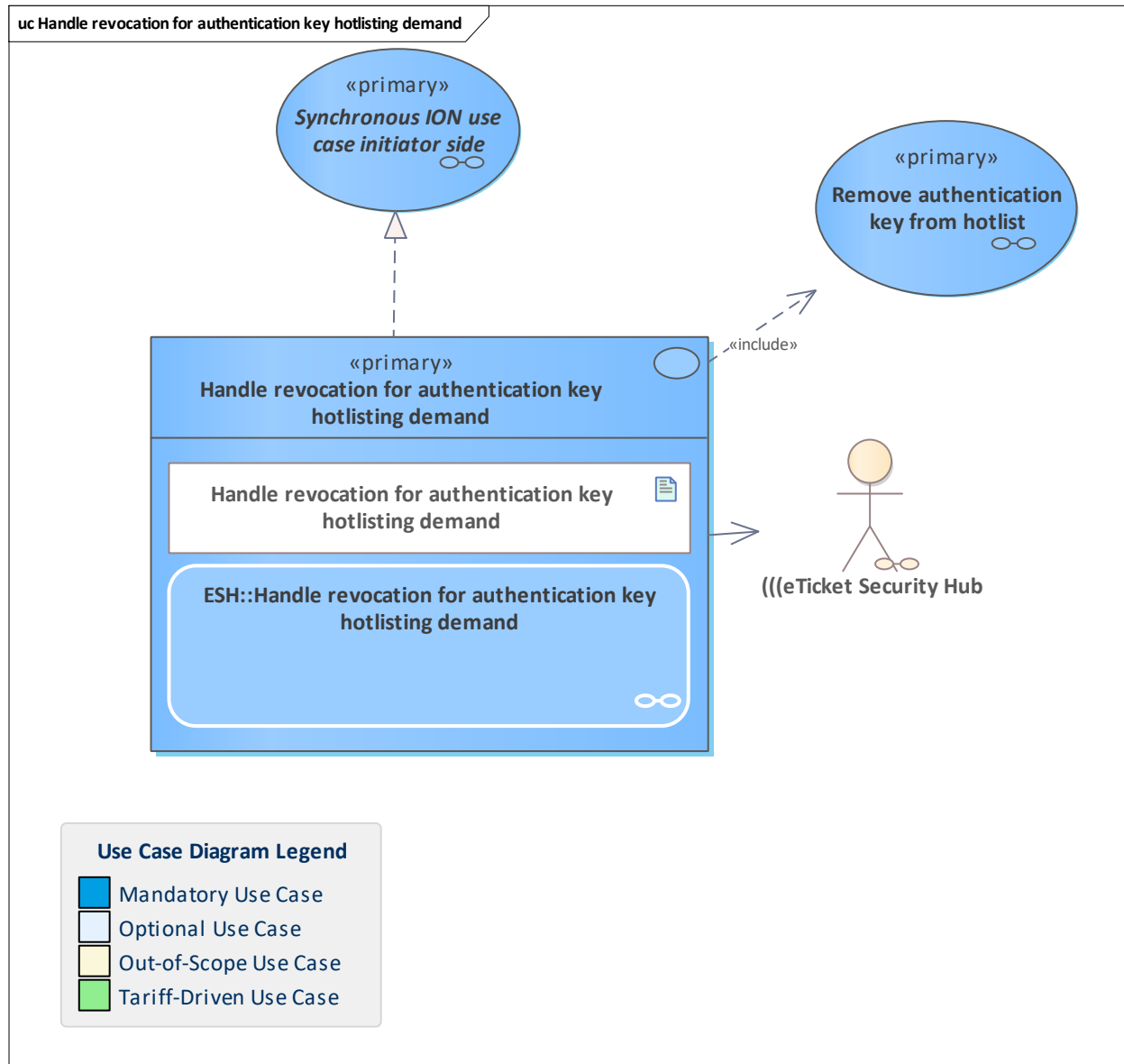


| | |
|-------------------------|--|
| Use Case | Handle authentication key hotlisting demand |
| Description | <p>Use case to add the current symmetric authentication key (for masterkey-based sessions between SAM and user medium). Either the demand for hotlisting authentication key has been received via the service management or the key usage period has expired. If the authentication key must be hotlisted, then the use case can be started.</p> <p>The scheme manager's ESH creates the request for adding the authentication key to the hotlist and sends it to the hotlist service system. The result will be updated in the ESH.</p> <p>Please note that authentication key hotlisting may have a huge impact on the ((etiCORE environment. Each terminal has to consider the entry in the hotlist and must get the SAM and user medium to use the next generation of the authentication key to establish the session.</p> |
| Initiating Actor | |
| Reacting Actor | (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |
| Linked Use Cases | |



| | |
|------------------------------------|--|
| (Extended By) | |
| Linked Use Cases (Includes) | Add authentication key to hotlist |
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |
| Inputs | |
| Outputs | |
| Error Cases | |
| Activity Diagram | ESH::Handle authentication key hotlisting demand |

2.2.2 Handle revocation for authentication key hotlisting demand

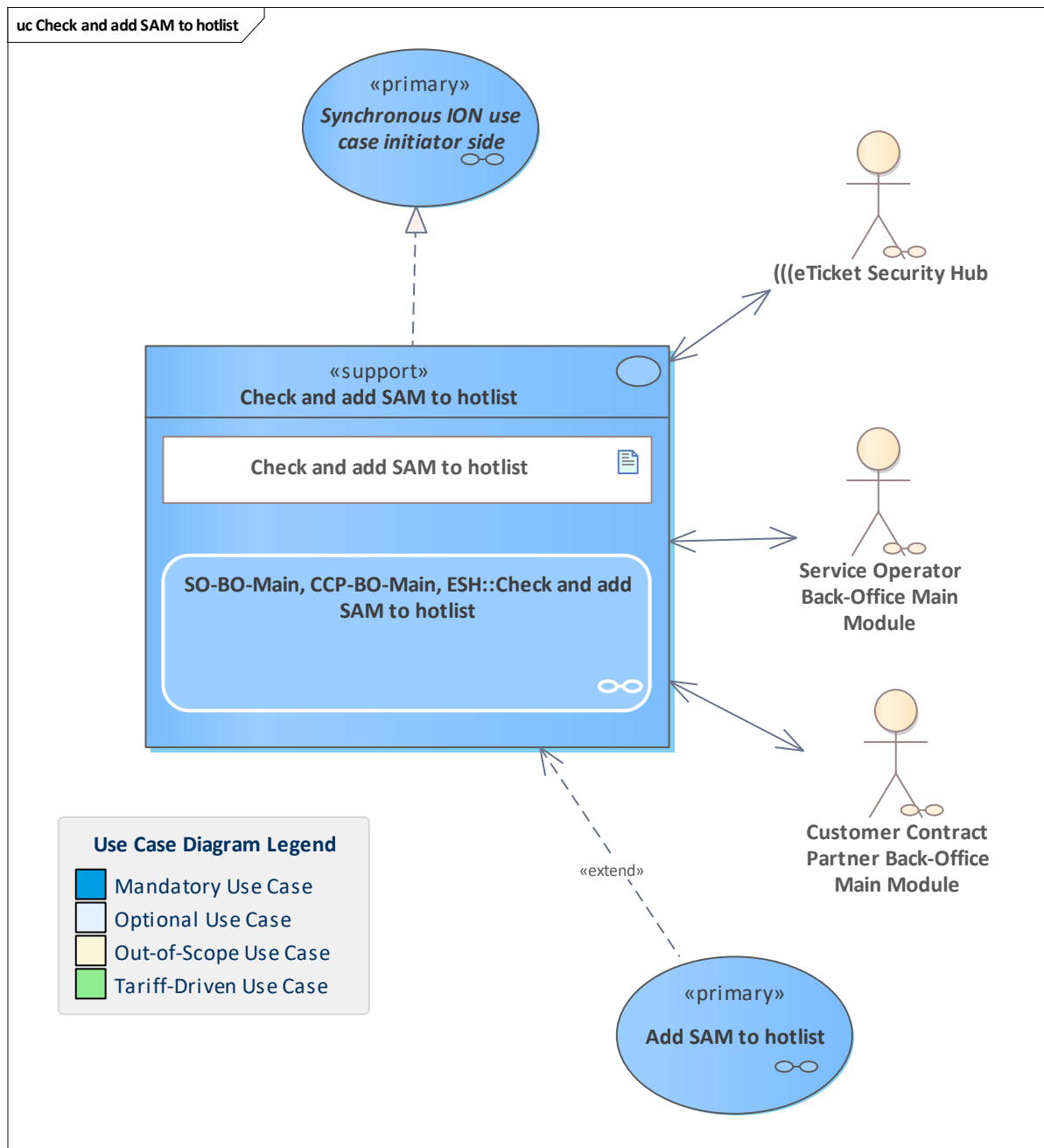


| | |
|-------------------------|---|
| Use Case | Handle revocation for authentication key hotlisting demand |
| Description | Rare use case only for the scheme manager's ESH. Authorised staff can remove an authentication key from the hotlist. This is only needed, if a new generation of user media or SAMs comes into play so that old authentication keys which are no longer placed on any UM or SAM can be removed. For this target, a request is sent to the hotlist service system to remove a certain authentication key from the hotlist. |
| Initiating Actor | |
| Reacting Actor | (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |



| | |
|---------------------------------------|---|
| Linked Use Cases (Extended By) | |
| Linked Use Cases (Includes) | Remove authentication key from hotlist |
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |
| Inputs | Authentication key to be removed from hotlist : SymmetricKeyId |
| Outputs | |
| Error Cases | |
| Activity Diagram | ESH::Handle revocation for authentication key hotlisting demand |

2.2.3 Check and add SAM to hotlist

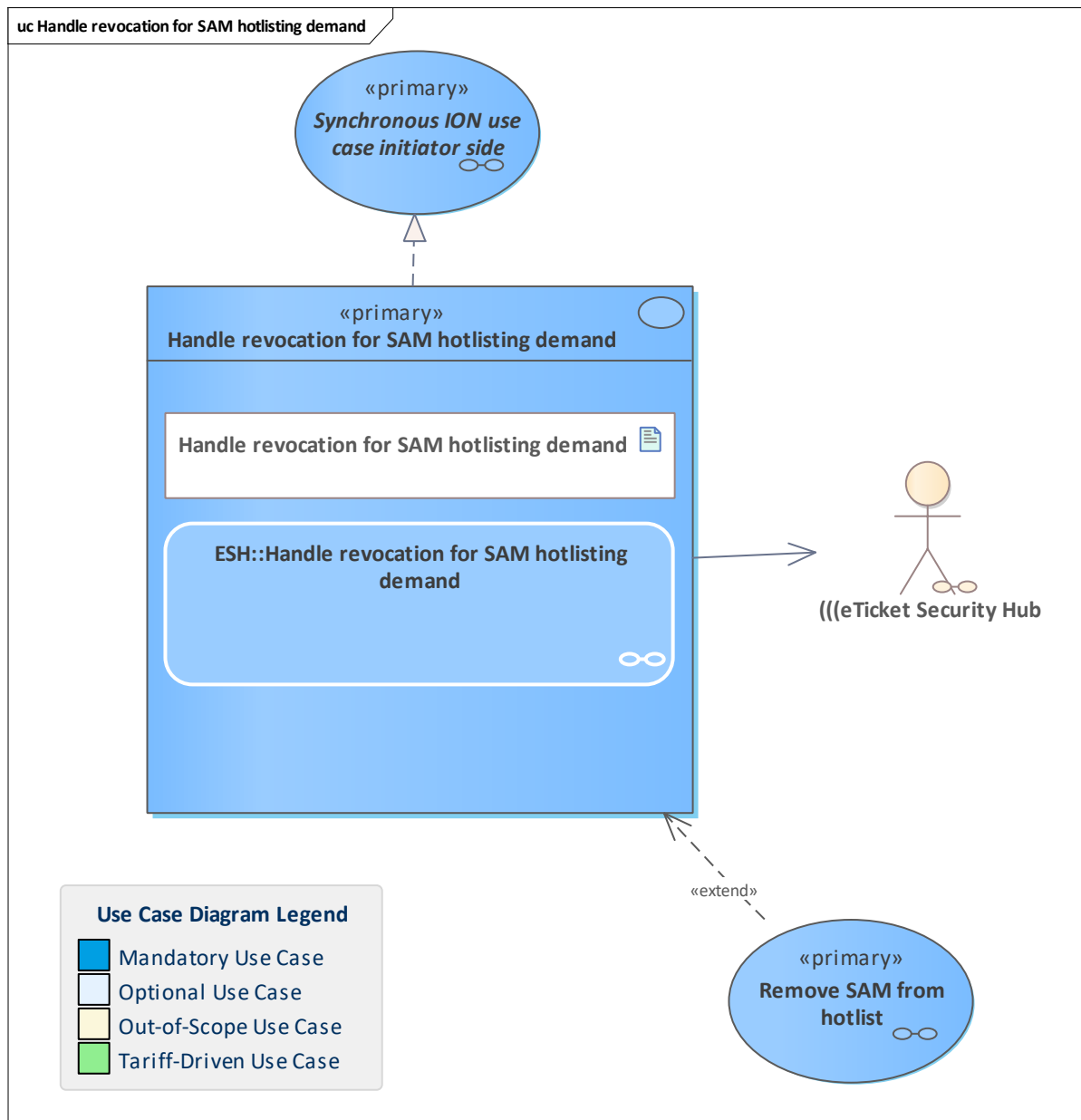


| Use Case | Check and add SAM to hotlist |
|-------------|---|
| Description | <p>Supporting use case for the Scheme Manager, SO or CCP.</p> <p>The parameters required to add a SAM to the hotlist are checked, especially if another system has already requested the SAM to be added to the hotlist.</p> <p>In addition, the SAM owner may add specific counter information that is not available to a third party system.</p> <p>The hotlist service system is requested to add the SAM to the SAM</p> |



| | |
|---------------------------------------|---|
| | hotlist. |
| Initiating Actor | (((eTicket Security Hub Service Operator Back-Office Main Module Customer Contract Partner Back-Office Main Module |
| Reacting Actor | (((eTicket Security Hub Service Operator Back-Office Main Module Customer Contract Partner Back-Office Main Module |
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | Add SAM to hotlist |
| Linked Use Cases (Includes) | |
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |
| Inputs | Blocking Reason : BlockingReason SAM action counter : ActionCounter SAM ID : AppInstanceId SAM entitlement issuance counter : EntitlementIssuanceCounter |
| Outputs | |
| Error Cases | |
| Activity Diagram | SO-BO-Main, CCP-BO-Main, ESH::Check and add SAM to hotlist |

2.2.4 Handle revocation for SAM hotlisting demand

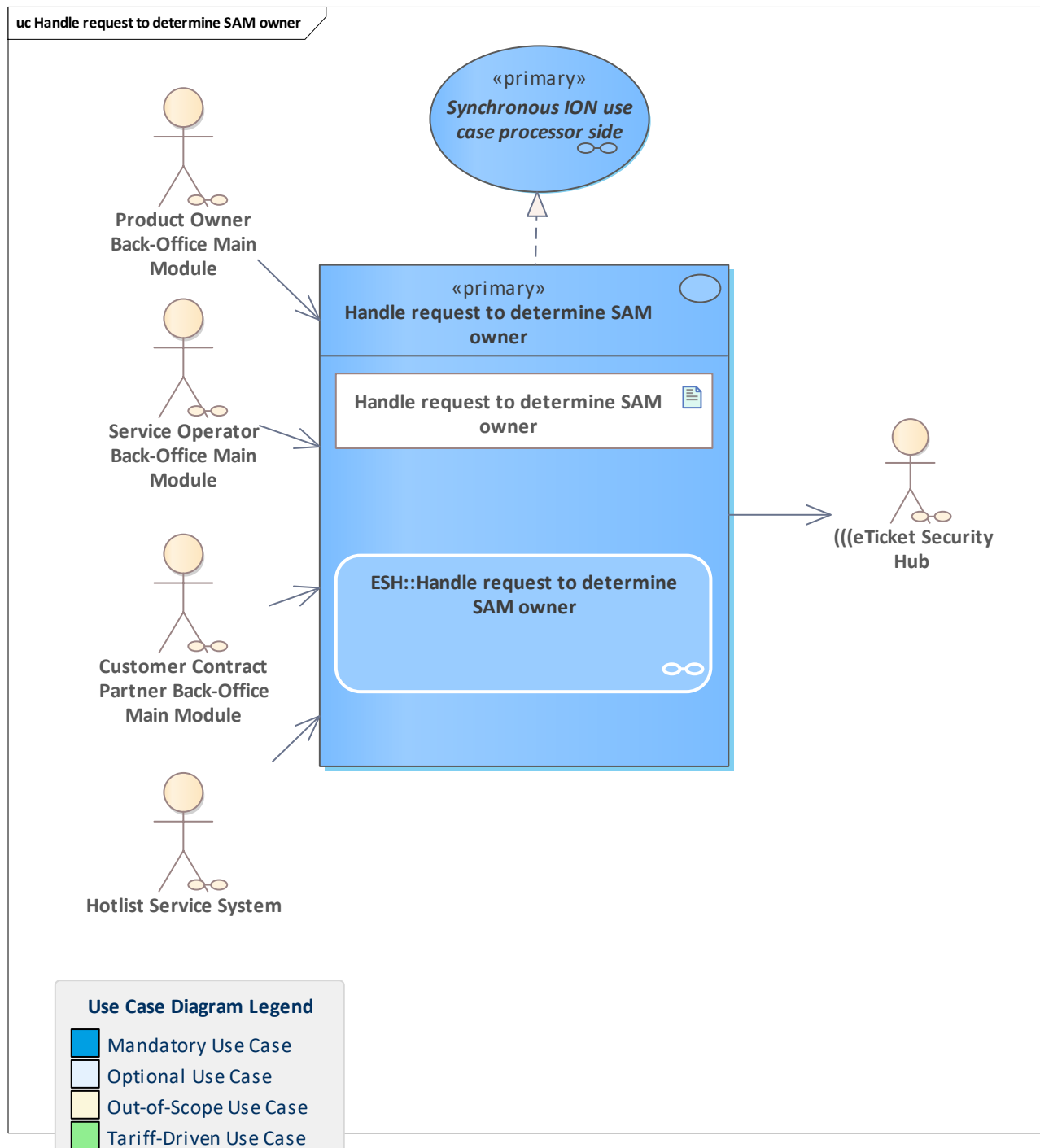


| | |
|---------------------------------------|---|
| Use Case | Handle revocation for SAM hotlisting demand |
| Description | In this rare use case, the scheme manager's ESH requests to remove the SAM from the hotlist, as a result of internal checks (e.g. SAM is more than 10 years on the hotlist or the SAM owner has provided proof of scrapping). |
| Initiating Actor | |
| Reacting Actor | (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | Remove SAM from hotlist |
| Linked Use Cases | |



| | |
|------------------------------------|--|
| (Includes) | |
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |
| Inputs | SAM ID : AppInstanceId |
| Outputs | |
| Error Cases | |
| Activity Diagram | ESH::Handle revocation for SAM hotlisting demand |

2.2.5 Handle request to determine SAM owner

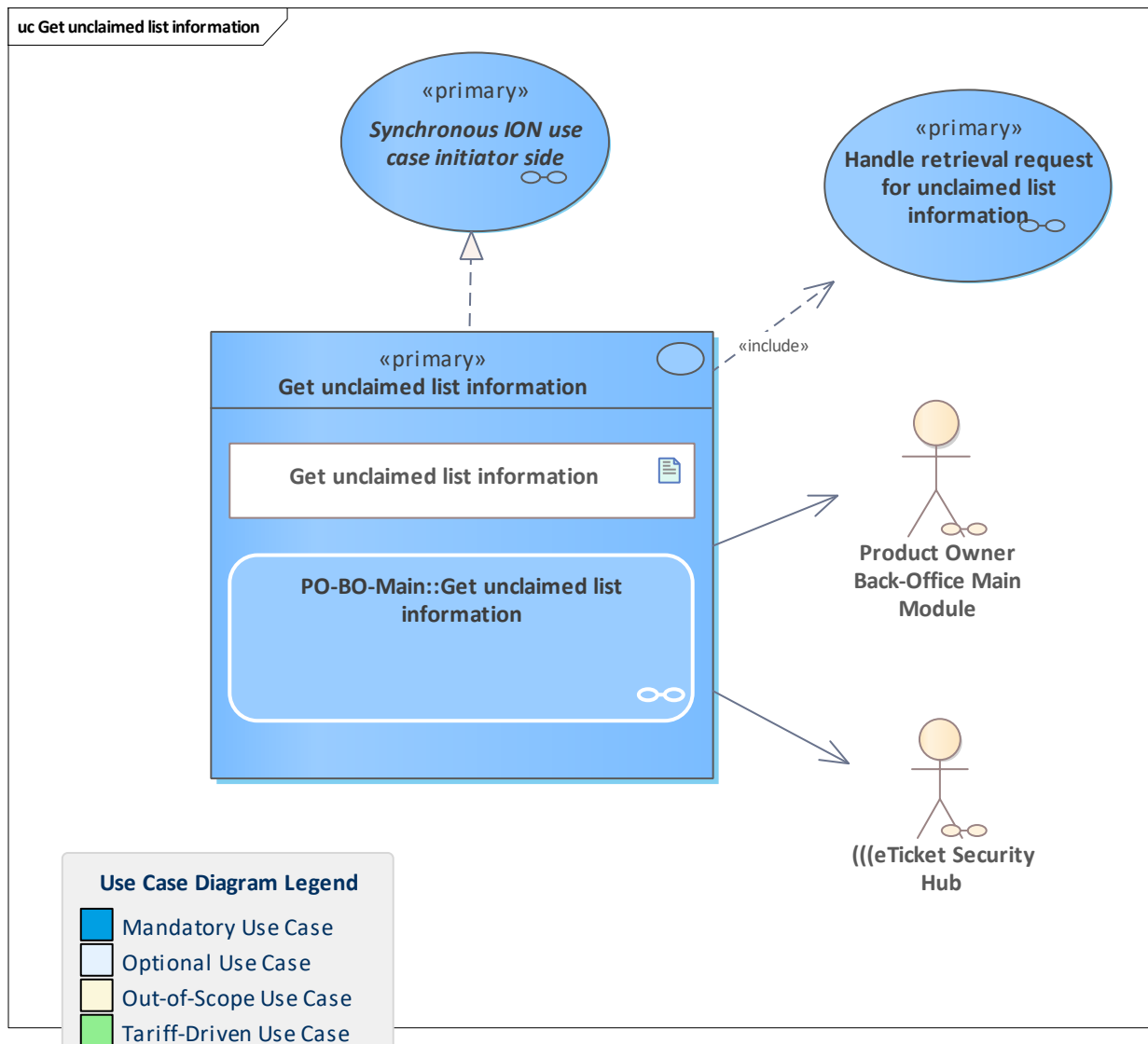


| | |
|-------------------------|--|
| Use Case | Handle request to determine SAM owner |
| Description | Provide the organisation ID and role of the SAM owner for a given SAM ID. |
| Initiating Actor | Product Owner Back-Office Main Module Service Operator Back-Office Main Module Customer Contract Partner Back-Office Main Module Hotlist Service System |
| Reacting Actor | (((eTicket Security Hub |



| | |
|---------------------------------------|---|
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | |
| Linked Use Cases (Includes) | |
| Linked Use Cases (Realises) | Synchronous ION use case processor side |
| Base Activity | |
| Inputs | Determine SAM owner : determineSAMOwner |
| Outputs | Determine SAM owner response : determineSAMOwnerResponse |
| Error Cases | E_CO_APP_INSTANCE_ID_UNKNOWN E_CO_WRONG_SECURITY_LEVEL Determine SAM owner exception : determineSAMOwnerException |
| Activity Diagram | ESH::Handle request to determine SAM owner |

2.2.6 Get unclaimed list information

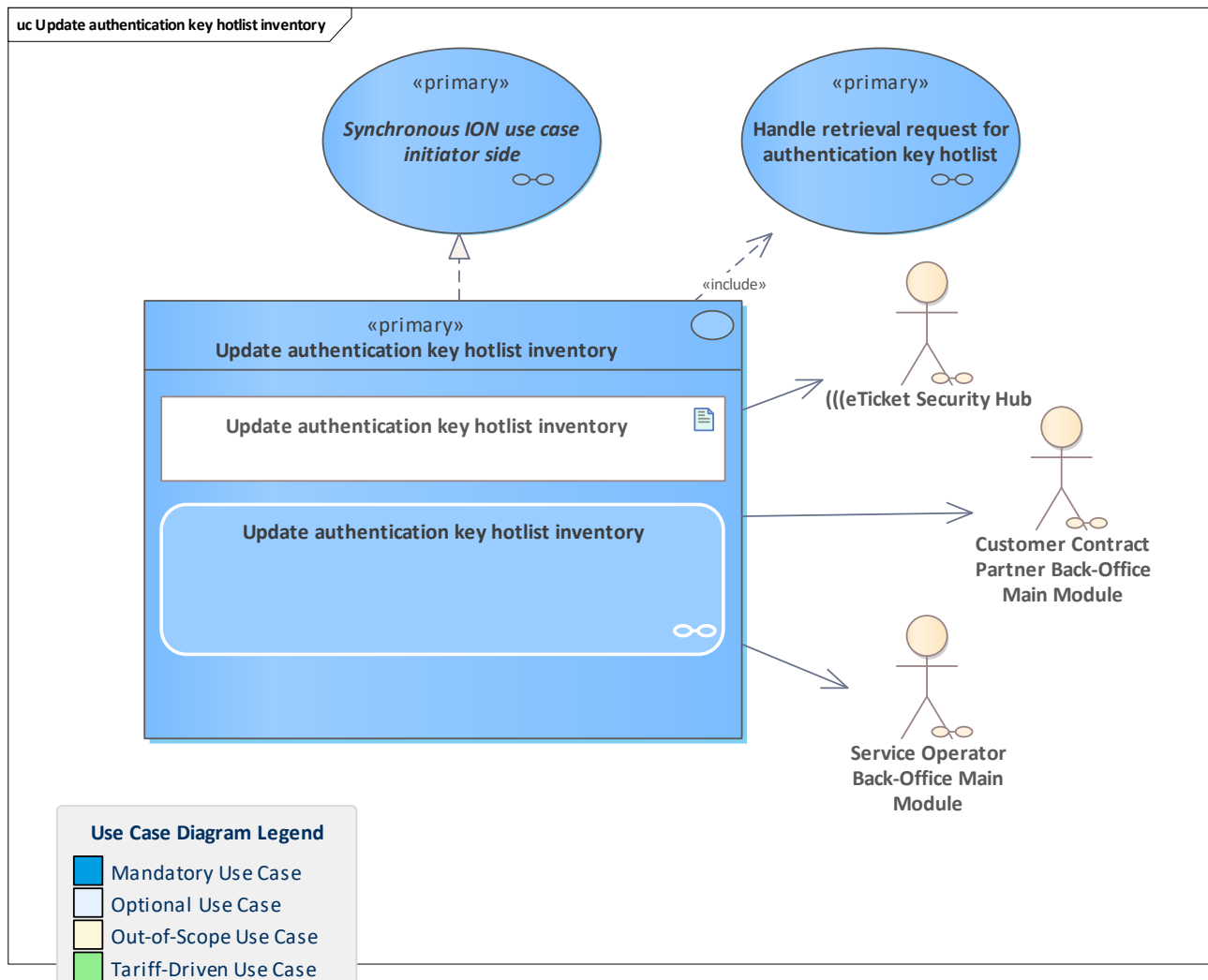


| | |
|-------------------------|--|
| Use Case | <u>Get unclaimed list information</u> |
| Description | <p>Use case that allows the PO to monitor the collection behaviour of its partner companies with the role SO and CCP. The scheme manager monitors all SO, CCP and PO organisations. The requestor gets the unclaimed list information from the hotlist service system for a period between the passed list cycle and the current list cycle. This information is registered and can be gathered for a regular report.</p> <p>The following list types are expected for the organisation's roles:</p> <ul style="list-style-type: none"> CCP and SO: application-, entitlement-, SAM-, organisation- and authentication-key-hotlist PO (included if the actor is the scheme manager): entitlement-, SAM- and organisation-hotlist |
| Initiating Actor | |
| Reacting Actor | <u>Product Owner Back-Office Main Module</u> <u>((eTicket Security Hub</u> |



| | |
|---------------------------------------|---|
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | |
| Linked Use Cases (Includes) | Handle retrieval request for unclaimed list information |
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |
| Inputs | List cycle number : ListCycleNumber |
| Outputs | |
| Error Cases | |
| Activity Diagram | PO-BO-Main::Get unclaimed list information |

2.2.7 Update authentication key hotlist inventory

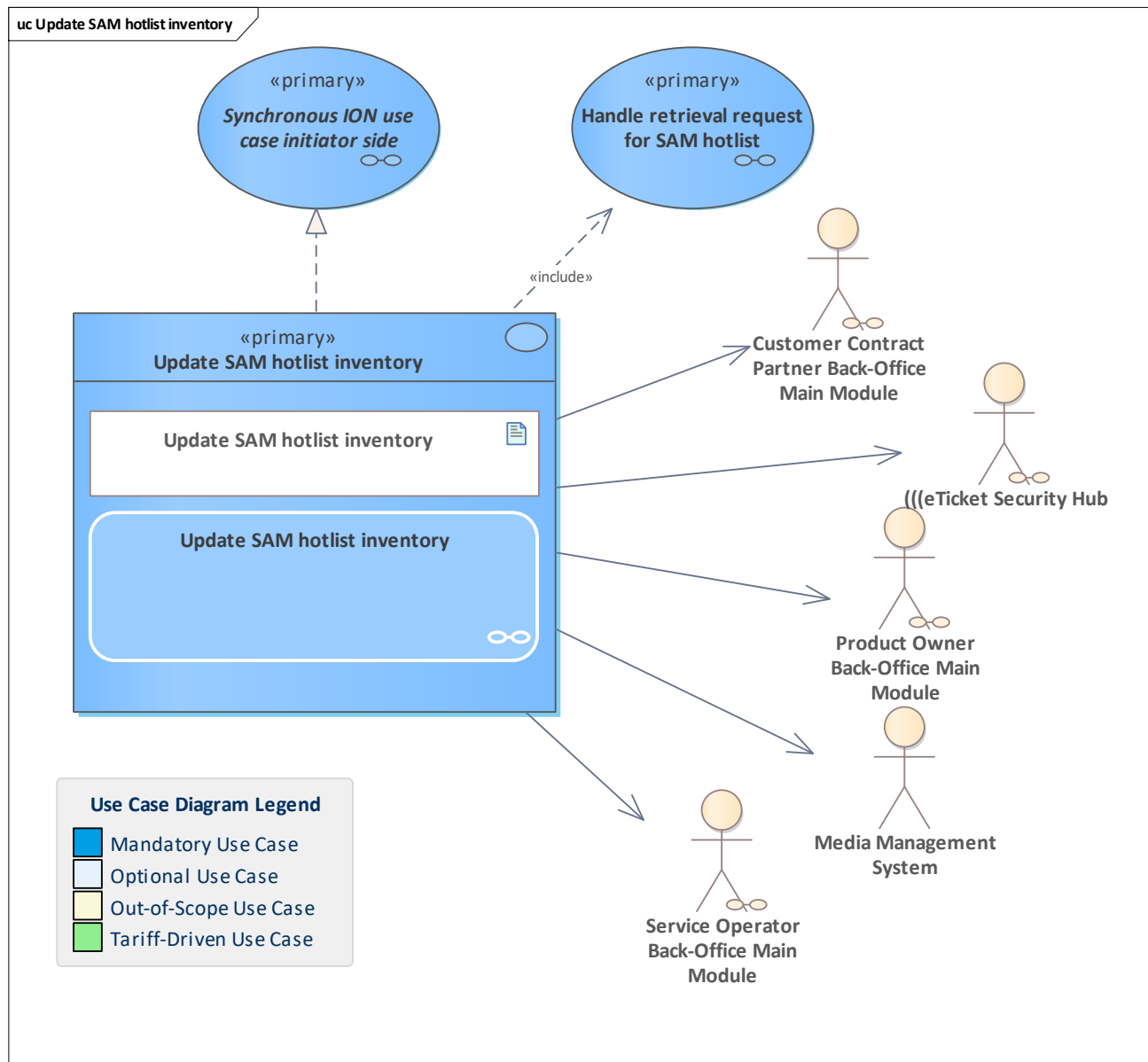


| | |
|---------------------------------------|--|
| Use Case | Update authentication key hotlist inventory |
| Description | The SO, CCP and the scheme manager's ESH want to update the authentication key hotlist inventory by retrieving the current authentication key hotlist from the hotlist service system and processing it into their authentication key hotlist inventory. |
| Initiating Actor | |
| Reacting Actor | Customer Contract Partner Back-Office Main Module Service Operator Back-Office Main Module (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | |
| Linked Use Cases (Includes) | Handle retrieval request for authentication key hotlist |
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |



| | |
|-------------------------|--|
| Inputs | |
| Outputs | Updated authentication key hotlist inventory |
| Error Cases | |
| Activity Diagram | Update authentication key hotlist inventory |

2.2.8 Update SAM hotlist inventory



| | |
|-------------------------|--|
| Use Case | <u>Update SAM hotlist inventory</u> |
| Description | The SO, CCP, PO and the scheme manager's ESH and MMS want to update their SAM hotlist inventory by retrieving the current SAM hotlist from the hotlist service system and processing it into the SAM hotlist inventory. |
| Initiating Actor | |
| Reacting Actor | Customer Contract Partner Back-Office Main Module Service Operator Back-Office Main Module Product Owner Back-Office Main Module Media Management System (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |
| Linked Use Cases | |



| | |
|------------------------------------|--|
| (Extended By) | |
| Linked Use Cases (Includes) | Handle retrieval request for SAM hotlist |
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |
| Inputs | |
| Outputs | Updated SAM hotlist inventory |
| Error Cases | |
| Activity Diagram | Update SAM hotlist inventory |



3 ESH Application Owner

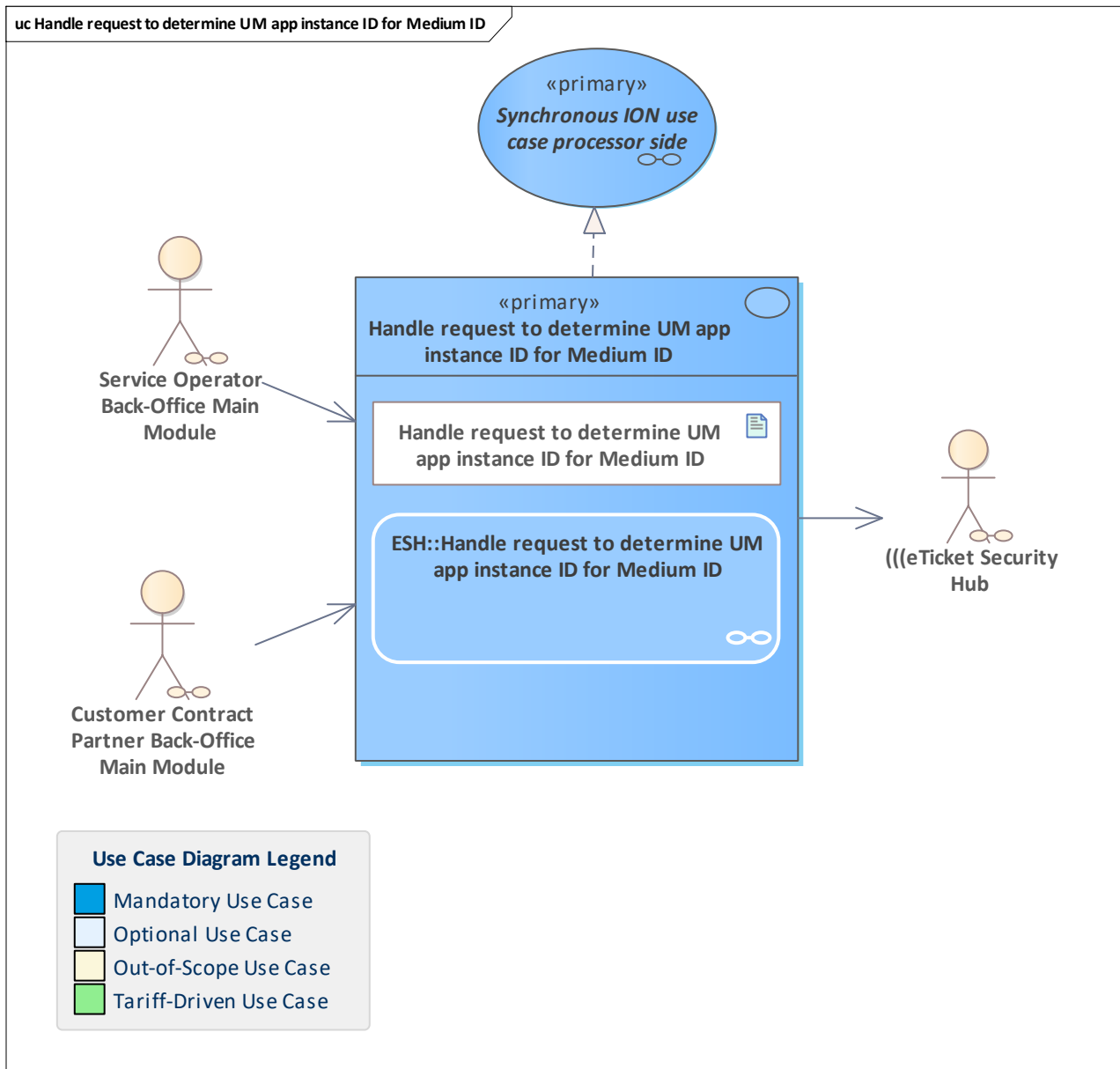
Functionality bundle that covers the use cases of the scheme manager as application owner.

3.1 Overview

Handle request to determine UM app instance ID for Medium ID
Terminate UM application

3.2 Use Cases

3.2.1 Handle request to determine UM app instance ID for Medium ID

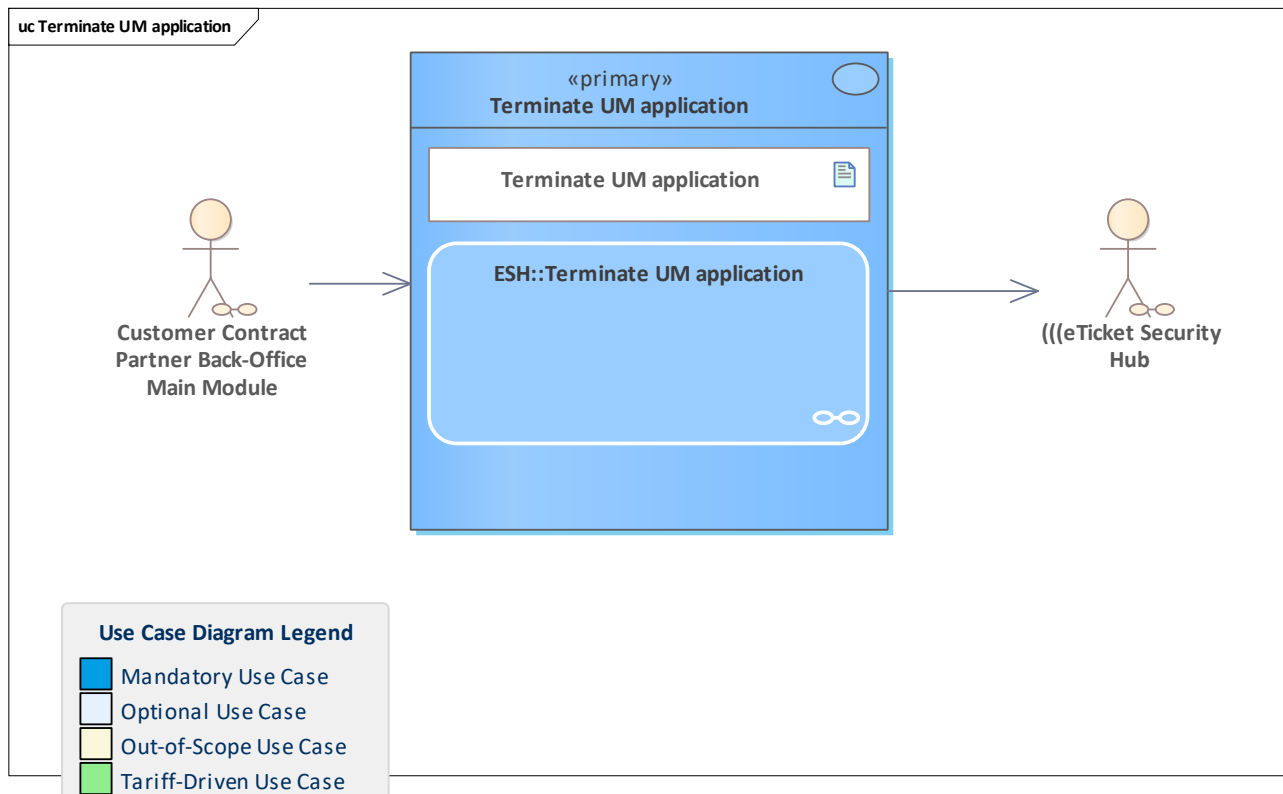


| | |
|---------------------------------------|---|
| Use Case | Handle request to determine UM app instance ID for Medium ID |
| Description | Provides the user medium application instance ID for a given medium ID. |
| Initiating Actor | Customer Contract Partner Back-Office Main Module Service Operator Back-Office Main Module |
| Reacting Actor | (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | |
| Linked Use Cases (Includes) | |
| Linked Use Cases (Realises) | Synchronous ION use case processor side |
| Base Activity | |



| | |
|-------------------------|--|
| Inputs | Get app instance ID for Medium ID : getAppInstanceIdForMediumId |
| Outputs | Get app instance ID for Medium ID response : getAppInstanceIdForMediumIdResponse |
| Error Cases | E ESH UNKNOWN MEDIUM ID Get app instance ID for Medium ID exception : getAppInstanceIdForMediumIdException |
| Activity Diagram | ESH::Handle request to determine UM app instance ID for Medium ID |

3.2.2 Terminate UM application



| | |
|---------------------------------------|--|
| Use Case | Terminate UM application |
| Description | This use case give participants the capability to inform the Scheme Manager about UM application terminations. Subsequently, the remaining certificate fees for the current application instance will be waived. |
| Initiating Actor | Customer Contract Partner Back-Office Main Module |
| Reacting Actor | (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | |
| Linked Use Cases (Includes) | |
| Linked Use Cases (Realises) | |
| Base Activity | |
| Inputs | Terminate UM application : terminateUmApplication |
| Outputs | Terminate UM application response : terminateUmApplicationResponse |
| Error Cases | E MMS REQUEST INVALID E MMS REQUEST DATA INVALID E MMS SIGNATURE INCORRECT E MMS MEDIUM UNKNOWN E MMS MEDIUM TERMINATED E MMS CA COMMUNICATION ERROR E MMS TECHNICAL ERROR |



| | |
|-------------------------|--|
| | Terminate UM application exception : terminateUmApplicationException |
| Activity Diagram | ESH::Terminate UM application |

4 ESH Registrar

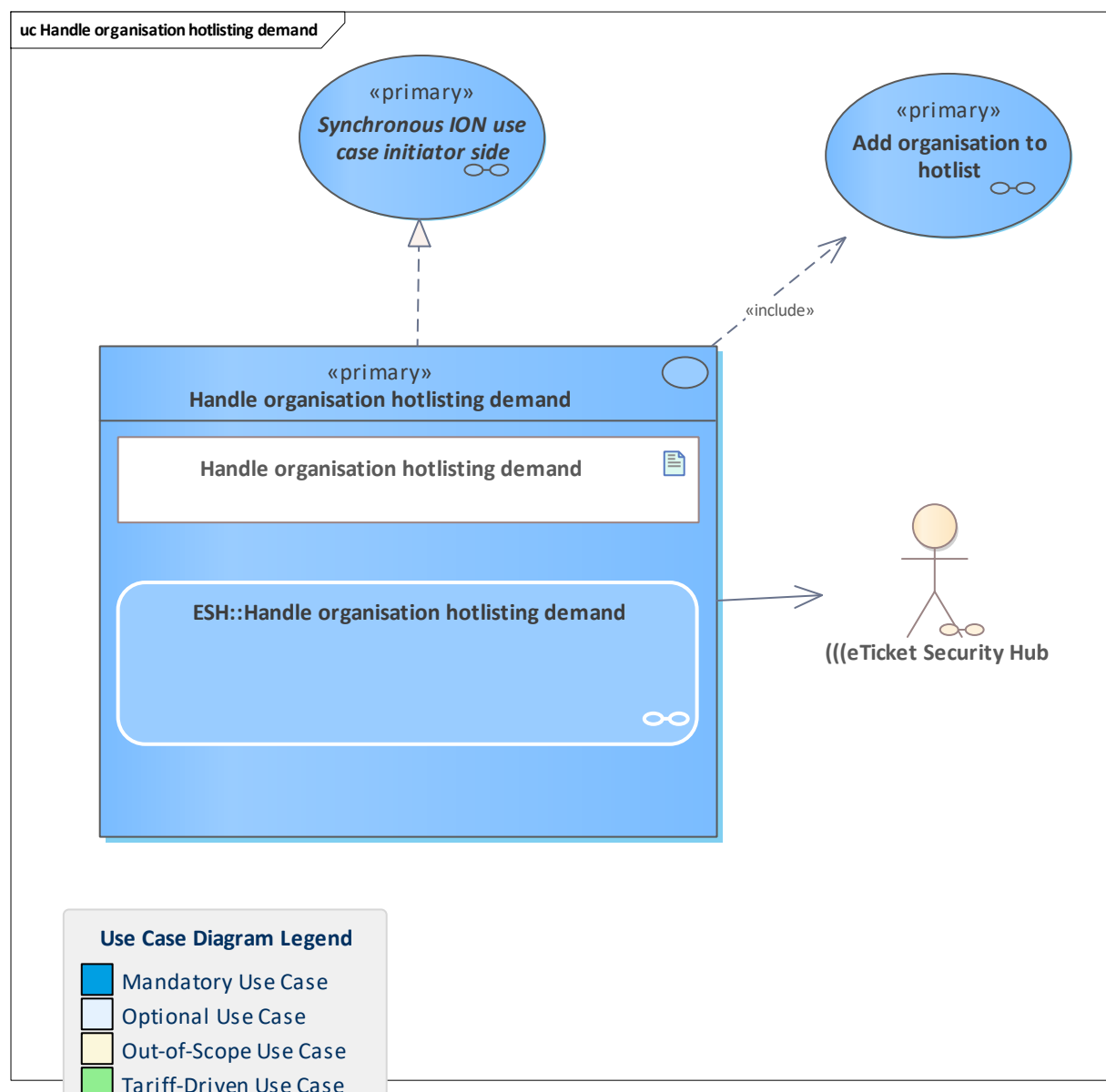
Functionality bundle that covers the use cases of the scheme manager as registrar.

4.1 Overview

Handle organisation hotlisting demand
Handle revocation for organisation hotlisting demand
Update organisation hotlist inventory
Process retrieval request for organisation list

4.2 Use Cases

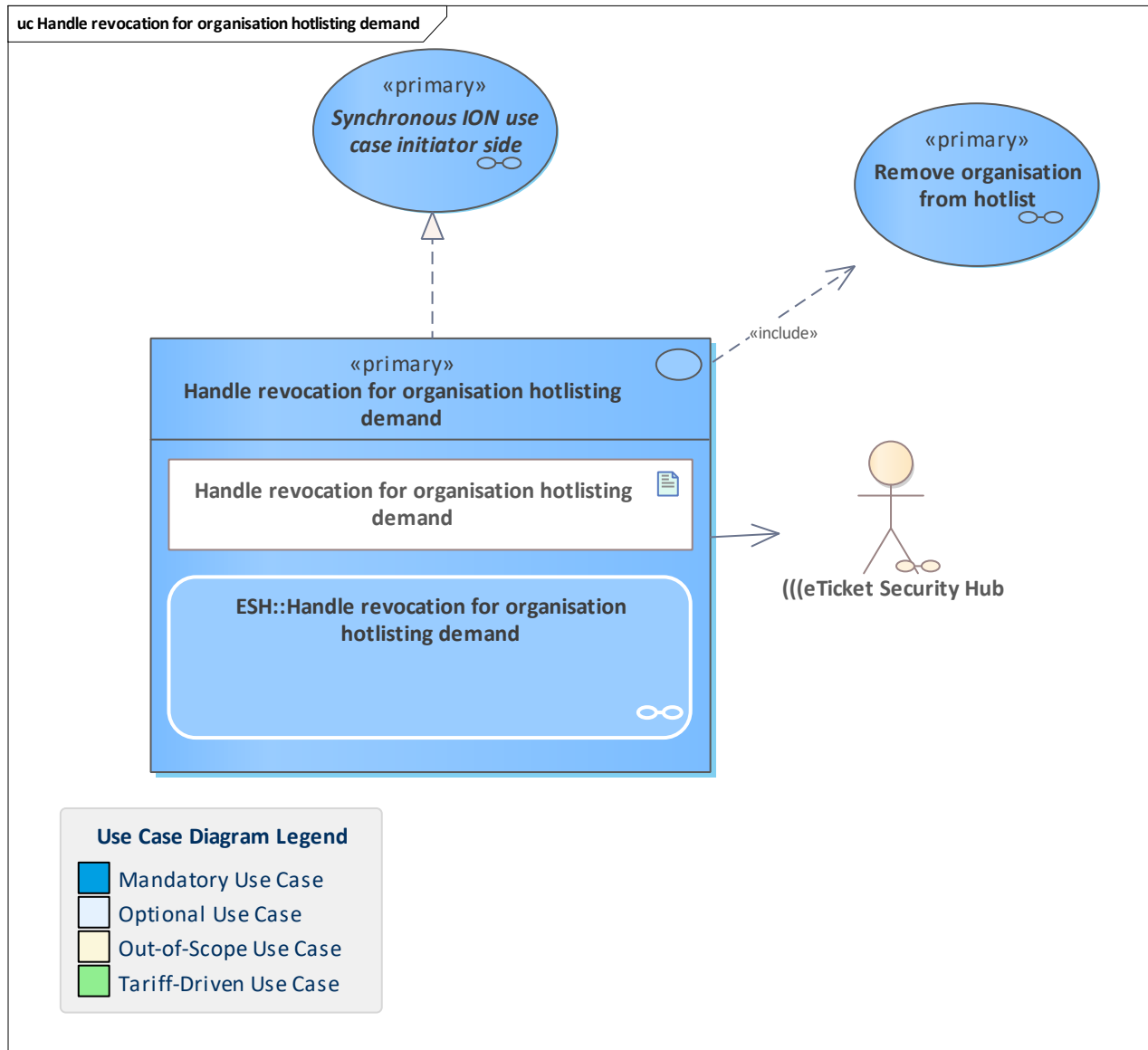
4.2.1 Handle organisation hotlisting demand





| | |
|---------------------------------------|---|
| Use Case | Handle organisation hotlisting demand |
| Description | <p>The demand for hotlisting an organisation has been received over the VDV-ETS service management or the organisation has to be hotlisted for other reasons.</p> <p>If the organisation must be hotlisted, then this use case can be started.</p> <p>In this use case, the request for adding the organisation to the hotlist is created and sent to the hotlist service system by the (((eTicket Security Hub (ESH) of the Scheme Manager. The result will be updated in the ESH.</p> <p>Note: hotlisting an organisation has a huge impact on the (((etiCORE environment, the SAMs of this organisation also have to be hotlisted. All involved applications and entitlements will be blocked by a terminal if the linked organisation ID is found on the hotlist.</p> |
| Initiating Actor | |
| Reacting Actor | (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | Add entitlement to hotlist |
| Linked Use Cases (Includes) | Add organisation to hotlist |
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |
| Inputs | Organisation Id : OrganisationId |
| Outputs | |
| Error Cases | |
| Activity Diagram | ESH::Handle organisation hotlisting demand |

4.2.2 Handle revocation for organisation hotlisting demand

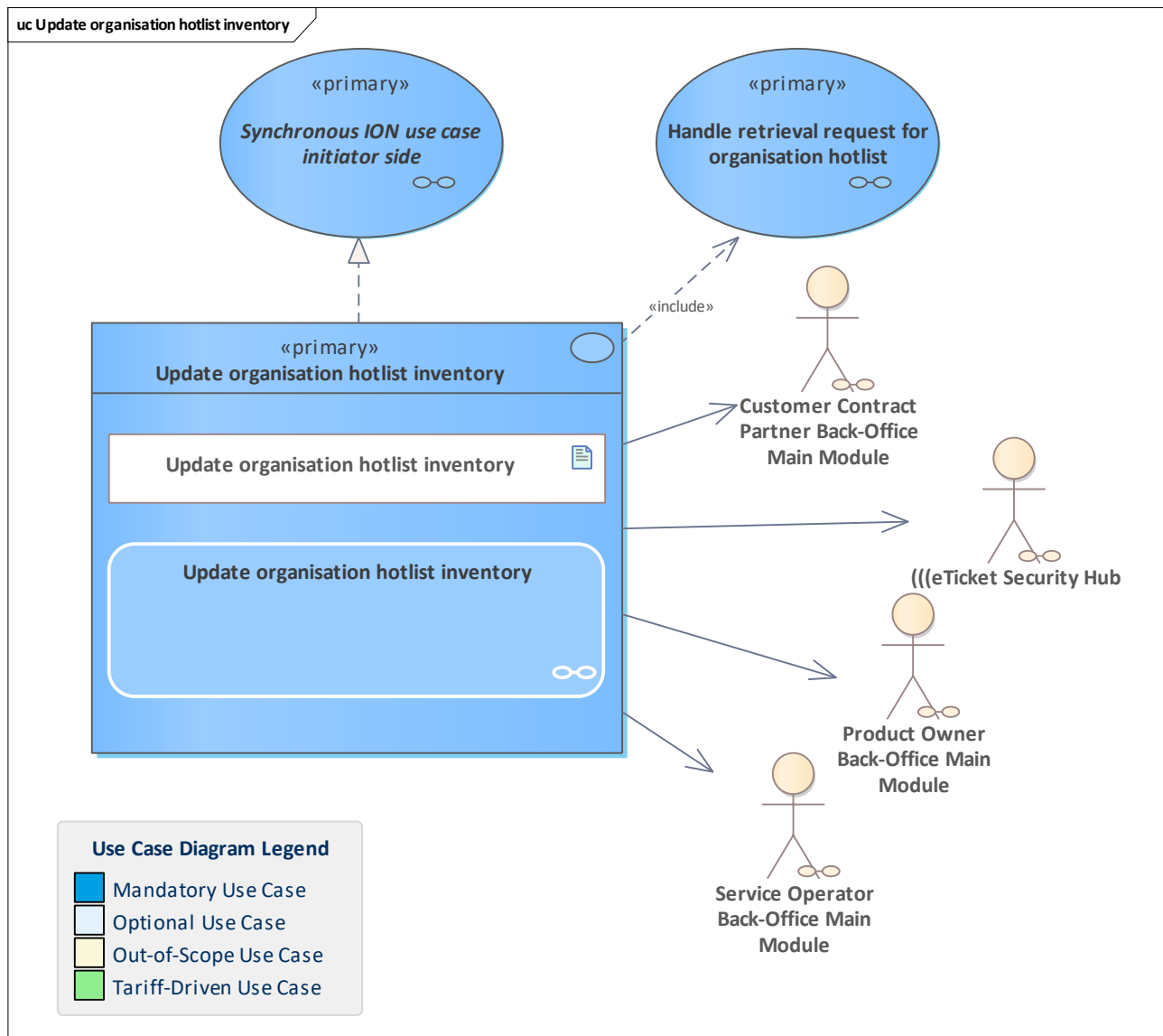


| | |
|---------------------------------------|---|
| Use Case | Handle revocation for organisation hotlisting demand |
| Description | For certain reasons, there may be no need to keep an organisation on the organisation hotlist (out of scope). In this rare use case, the Scheme Manager requests via the ESH to remove the organisation from the organisation hotlist. |
| Initiating Actor | |
| Reacting Actor | (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | |
| Linked Use Cases (Includes) | Remove organisation from hotlist |



| | |
|------------------------------------|--|
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |
| Inputs | Org ID of organisation to be removed from hotlist : OrganisationId |
| Outputs | |
| Error Cases | |
| Activity Diagram | ESH::Handle revocation for organisation hotlisting demand |

4.2.3 Update organisation hotlist inventory

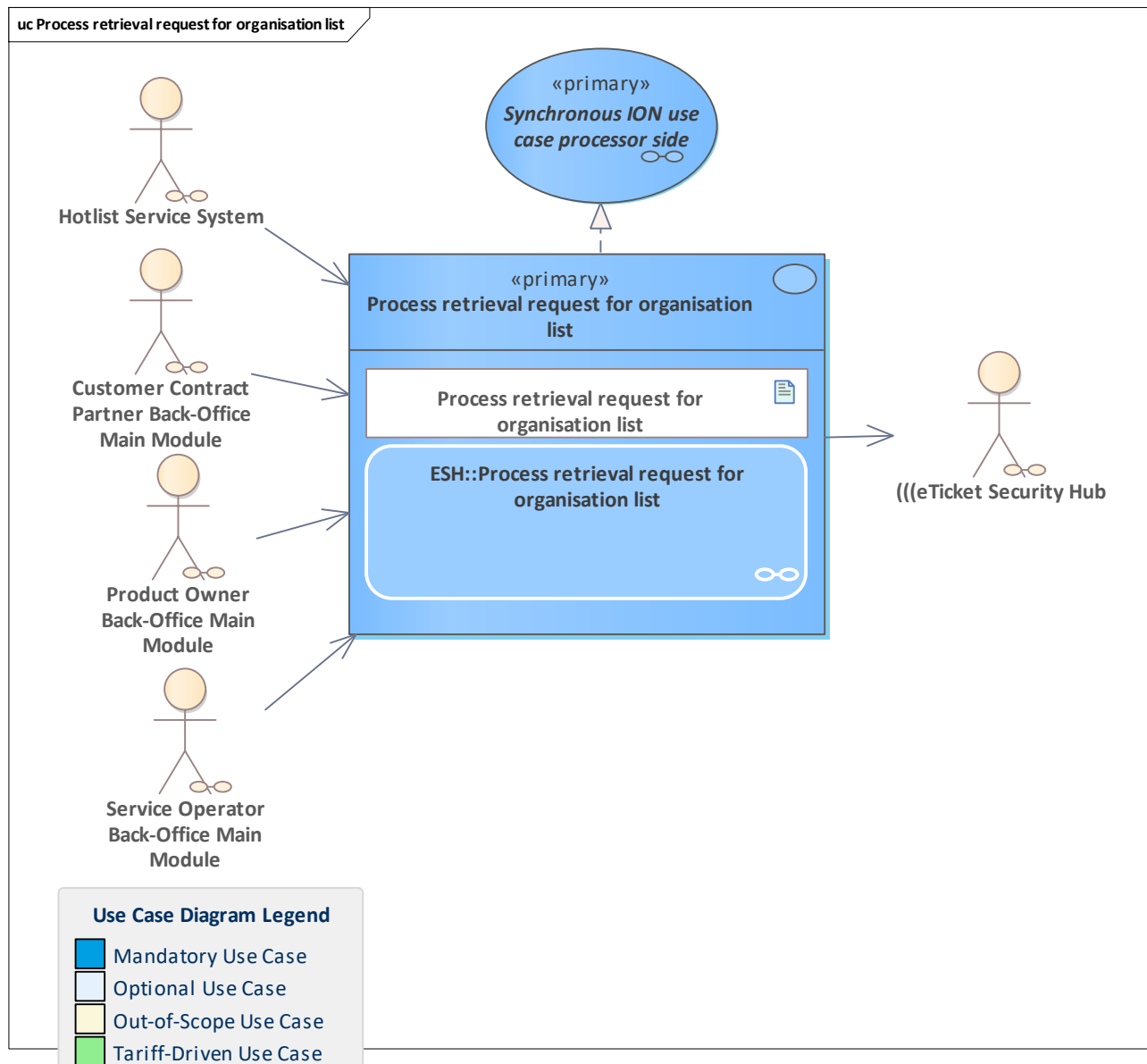


| | |
|---------------------------------------|--|
| Use Case | Update organisation hotlist inventory |
| Description | The SO, CCP, PO and the scheme manager's ESH want to update their organisation hotlist inventory by retrieving the current organisation hotlist from the hotlist service system and processing it into their organisation hotlist inventory. |
| Initiating Actor | |
| Reacting Actor | Customer Contract Partner Back-Office Main Module Service Operator Back-Office Main Module Product Owner Back-Office Main Module (((eTicket Security Hub |
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | |
| Linked Use Cases | Handle retrieval request for organisation hotlist |



| | |
|------------------------------------|---|
| (Includes) | |
| Linked Use Cases (Realises) | Synchronous ION use case initiator side |
| Base Activity | |
| Inputs | |
| Outputs | Updated organisation hotlist inventory |
| Error Cases | |
| Activity Diagram | Update organisation hotlist inventory |

4.2.4 Process retrieval request for organisation list



| | |
|---------------------------------------|--|
| Use Case | <u>Process retrieval request for organisation list</u> |
| Description | The registrar creates an organisation list and sends it to the requestor. |
| Initiating Actor | <u>Hotlist Service System</u> <u>Customer Contract Partner Back-Office Main Module</u> <u>Product Owner Back-Office Main Module</u> <u>Service Operator Back-Office Main Module</u> |
| Reacting Actor | <u>(((eTicket Security Hub</u> |
| Preconditions | |
| Postconditions | |
| Linked Use Cases (Extended By) | |
| Linked Use Cases (Includes) | |
| Linked Use Cases | <u>Synchronous ION use case processor side</u> |



| | |
|-------------------------|--|
| (Realises) | |
| Base Activity | |
| Inputs | Get organisation list : getOrganisationList |
| Outputs | Get organisation list response : getOrganisationListResponse |
| Error Cases | Get organisation list exception : getOrganisationListException |
| Activity Diagram | ESH::Process retrieval request for organisation list |

