Project:	
Module:	**Flag Management**
Submodule:	**SIB/CUD Flag**
Entry document:	**Work Order**
Current version:	**100727-1.0**
Initialization documents:	1. Initial documents\13_DTS Release 1_32\DTS-Releasev1.32\DTS1.32\Concepts\sisii-flagging. V1.19.doc 2. Initial documents\10_Detailed system specifications\SINS-PMI-SDSis-v1.2-RO-SpecificatiiDetaliateDeSistem.doc/pg.61-Flagging 3. Initial documents\6_Modelul CU use cases\SINS-PMI-RInSW-v1.3-RO-Report Initial Analysis SINS-Software-Modelul CU_PL (431p).doc\pg. 205-211 3. Initial documents\7_Definition of the Application Model/pg.22-24.
Reference documents:	

Version	Author
100616-1.1	Andrei Popovich

Content:

1. Description of the work topic

1.1 General view

(ref. Initialization documents/1/pg. 7)

SISII is primarily a hit-no-hit information system, allowing National States in Europe to share information on alerts they have issued. Thus, the maintenance and management of alerts builds the core business functionality of the system. This concept entails all the operations necessary to maintain and manage flags, which is another crucial functionality of the Schengen Information System.

Flagging refers to a process already implemented in the current system (SISI+). It allows a Contracting Party (ie a User), in accordance with the rules and regulations of the Schengen Convention and the procedures described in the SIRENE Manual, to indicate that it will not follow the action specified in an alert issued by another Contracting party (from here on referred to as the role alert owner or alert

issuer). This is due to restrictions imposed by its national legislation. Flagging is part of the alert management.

In some cases the contracting party requesting the flag (from here on referred to as the role flag requester) can specify an alternative action. In other cases, however, a validity flag implies that the "Action to be taken" for the alert in question cannot be followed by the flag requester. There is a strong connection between the alert life cycle (see [Concept SIS II Alert Maintenance [45]] and [Concept SIS II Business Services [72]]) and flagging life cycle. Although flags are a separate class, flags still belong to the corresponding alert. Therefore, if an alert will be deleted all flags belonging to this alert have to be deleted accordingly. The flag will be added to the history if a flag is added to an alert or changed.

According to the current version of the Legal Basis and the SIRENE Manual only the alert owner is allowed to create, delete, etc. flags for his alerts due to the request of a flag requester (Business Rule: The owner of a flag is the owner of the corresponding alert). The possibility that in the future only the flag requester (who then will be the flag owner) will be able to use the Business Services for flagging has been foreseen in the analysis and design of SIS II (Business Rule: The owner of the flag is the requester of the flag).

It is technically possible to easily include this feature by adopting the applicable business rules in the subsystem Business Services (see concept [Concept SIS II Business Services [72], chapter 5.2.1, 5.2.2, 5.2.3 and 5.2.4]) and subsystem "Broadcasting and Notification" (see applicable concept [Concept SIS II Broadcast and Notification [47]]).

The flagging process comprises all the processes and functions involved in the management of flags like:

- create flag
- update flag
- delete a flag

Operations concerning Flags are strictly speaking also part of Alert Maintenance. For readability's sake further information and requirements regarding alert maintenance operations, having an impact on flags, can be found in [Concept SIS II Alert Maintenance [45]].

It should be noted that there are several logically (in some cases physically) separate data pools in which Information about flags is stored:

- the operational data ie the information available for the day-to-day business processes
- the historical data, available for immediate revision of the flag history
- the logs, intended to support auditing

The operations, statuses, and requirements described in this concept relate solely to the maintenance of flags in the operational data pool.

Information, requirements and the relevant operations regarding the logging and history of flags can be found in [Concept SIS II History Log [51]] and [Concept SIS II Logging [53]].

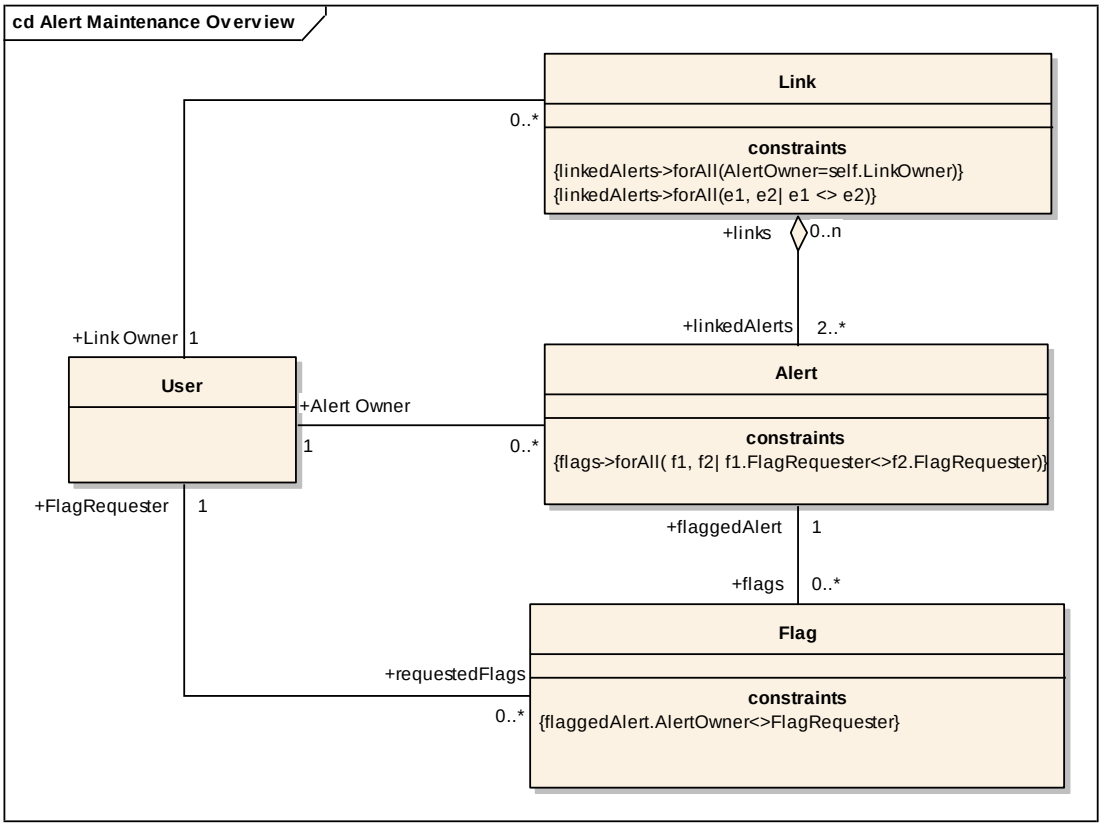


Fig.1- Signal management-Overview (ref. Initialization Documents/1/pg. 13)

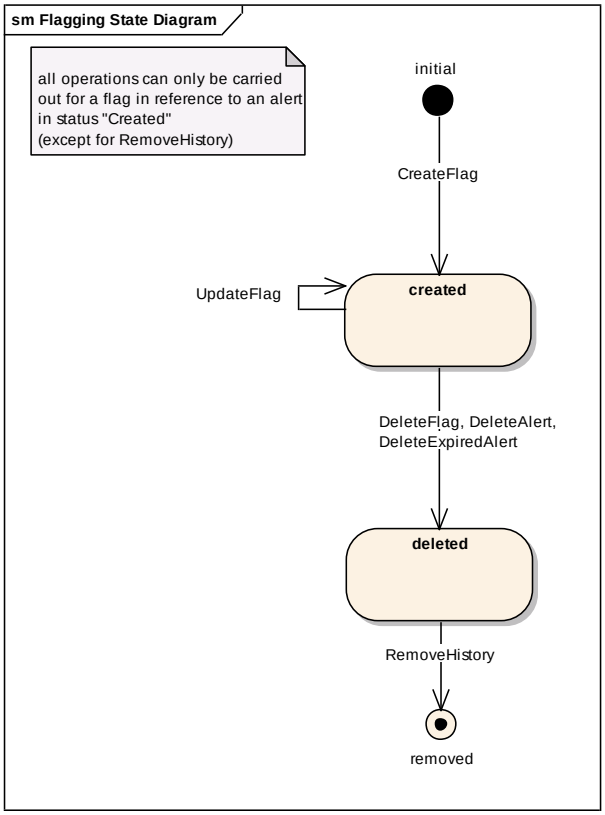
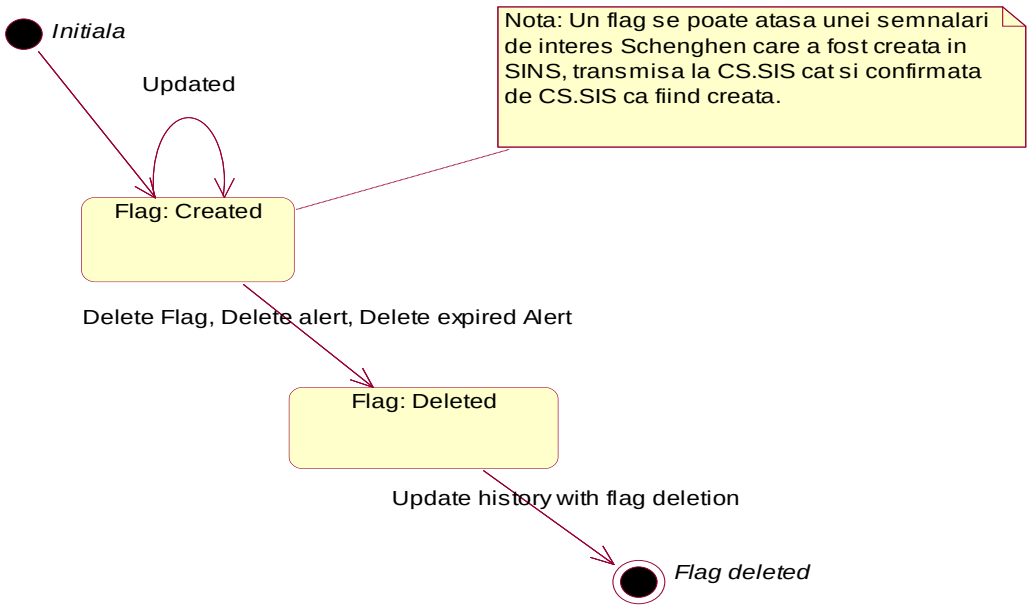


Fig. 2 – State diagram of a Flag object (ref. Initialization Documents/1/pg. 14)



The diagram shows the overview of the life cycle of a flag in terms of operations and resulting states.

condition	Trigger event	Actions that can be taken	Remarks
Initial	The user of the national SIRENE Bureau, at the request of a member state, attaches a flag to a Romanian alert of Schengen interest that was previously successfully transmitted to CS.SIS.	No actions can be taken in this state	Since it is not known whether the flag data has been successfully transmitted to CS.SIS, the Flag is not available for modification or deletion.
Flag Created	Receiving the response from CS.SIS that the flag was created successfully.	The only actions that can be taken in this state are to change the flag or delete the flag.	The flag introduced by the national SIRENE Bureau at the request of another member state is not displayed in searches carried out at the level of SINS or CS.SIS National Copy.

condition	Trigger event	Actions that can be taken	Remarks
Flag Deleted (final state)	The flag is deleted by the user of the national SIRENE Bureau at the request of the Member State that requested its creation. The flag is deleted when the flag to which it is attached is deleted (as a result of a HIT, an error or expiration).	No actions can be taken in this state	A deleted flag cannot be recovered. The deletion operation is logged. Once the flag is deleted, its related history is also closed. Information about the history of the flag is displayed in the history of the flag to which it was attached.

2. IT design- Flagging

2.1. Status tables need to be implemented in programmed logic

Features / Status	Initial	Created	Deleted	Removed
They exist physically in the database		X	X	
It exists in the operational data pool		X		
It exists in the history data pool		X	X	
I am in logging data		X	X	X
Must exist in operative NS-SIS with NC		X	N/A	
Accessible on-line ie retrieve/read		X	X	
Responds to ALL queries		X		
Considered in the Report		X	X	
Data Consistency Check		X	(X)*	

* The flag histories in the central and national data bases will not be compared, however, the data consistency process makes use of the alert history (please see [Concept SIS II Data Consistency [48]])

Table1: Characterization of the states of the Flag object and associated characteristics

Operation / Status	Initial	Created	Deleted	Removed
CreateFlag operation	X			
UpdateFlag operation		X		
DeleteFlag operation		X		
Operation DeleteAlert		X		
Operation DeleteExpiredAlerts		X		

Operation RemoveHistory			X	

Table2: Characterization of the states of the Flag object and associated operations

2.2. Flagging use case

1.1.1 USE CASE: 09 ADD FLAG TO A SIGNAL

Use case ID: 09

Use case name: Add Flag to Signaling

Range:

Use Case "**Adding Flag to Signaling", as part of the Use Case Diagram, describes the functionality of adding a flag to a Romanian signal of Schengen interest that has been sent to CS.SIS.**

The flag applies only to the signals from Article 6 letter a and Article 6 letter b according to the legislation in force and for signals related to discrete control.

Subsystem:

WEB	WAP	Message queues	WEB Services	FTP/SCP
YES	NOT	**YES**	NOT	NOT

Description:

The purpose of the Use Case is to add a flag to an existing signal of Schengen interest belonging to the Romanian state that has been successfully transmitted to CS.SIS. The flag is attached to an alert only at the request of another Member State, by the authorized user of the national SIRENE Bureau.

Business Events:

The SIRENE Bureau of a member state requests the national SIRENE Bureau to apply a flag to a Schengen alert of interest belonging to the Romanian state.

Actors:

- The SIRENE Bureau through the SIRENE officer who has the right to apply a flag to an existing alert of Schengen interest belonging to the Romanian state
- Data provider system (national SIRENE Bureau system)

Prerequisites:

- The data provider system is operational
- The SINS system is operational
- The access interface to SINS is operational
- The user is authenticated in SINS and in the data provider system (National SIRENE Bureau System) and has the right to attach a flag to an existing alert
- The data provider system has all the necessary elements (at least the minimum mandatory information) for creating the flag
- The alert to which the flag must be applied is an alert of Schengen interest and has been sent to CS.SIS.

Main Scenario –**Adding a flag to an existing alert from message queues (in the case of the modernized IT system of the National SIRENE Bureau)**

Step	Data provider system (National SIRENE Bureau System)	MEANING
1	The data provider system authenticates.	
2		SINS verifies the authentication credentials and access rights related to the Data Provider System. **UC 00.01 National System authentication in SINS.**
		If the credentials of the provider System have been verified successfully, proceed to step 3.
3	The provider system generates the request to add a flag to a signal and includes it in a message. The system places the message in its own output queue.	

4		SINS retrieves the message from the output queue of the Data Provider System.
5		SINS logs the request to add a flag to a flag.
6		SINS verifies the credentials of the user who requested the addition of the flag to a flag in the Provider System. UC 00.02 – User authentication/authorization in SINS
		If the User who requested the addition of the flag to a signal in the provider system successfully authenticates, then proceed to step 6.
6		SINS validates the structure of the received message by checking whether it complies with the validation scheme
7		If the message is valid the use case continues from step 14, otherwise from step 8.
8		SINS generates a confirmation message that explicitly indicates the reason for the invalidation.
9		SINS places the confirmation message in the input queue of the data provider System that sent the request.
10		SINS logs the confirmation on the request to add a flag to an existing flag (successful, unsuccessful).
11	The provider system takes the confirmation message from its own input queue and processes it.	
12		The use case is completed by the error message.
13		SINS logs the confirmation on the request to add a flag to an existing flag (successful, unsuccessful).

14		SINS validates the request to add a flag to an existing flag according to the defined business rules.
15		If all business conditions are met the use case continues from step 21, otherwise from step 16.
16		If the request to add a flag to an existing signal transmitted through the message does not comply with the defined business rules, SINS generates a confirmation message that explicitly indicates the reasons for the invalidation and any warnings if any.
17		SINS places the error message in the input queue of the Data Provider System that submitted the request.
18		SINS logs the confirmation of the request to add a flag to an existing flag (successful, unsuccessful)
19	The provider system takes the confirmation message from its own input queue and processes it.	
20		The use case is completed by the confirmation message to the request to add a flag to an existing flag (successful, unsuccessful).
21		The flag is created in SINS by entering all the information in the database.
22		SINS logs the operation of adding a flag to an existing flag.
2. 3		SINS makes the flag available for other operations.
24		SINS creates a confirmation message. The message may also contain warning messages resulting from the verification of business rules. SINS places the message in the input queue of the Data Provider System.

25		SINS logs the response to the create flag request.
26	The provider system takes the confirmation message from its own input queue and processes it.	

Alternative scenario –**Adding a flag to an existing flag through the web interface**

Step	Delegated user of the Data Provider System (National SIRENE Bureau)	MEANING
1	The user logs in.	
2		SINS checks the credentials of the user who wants to connect to the UC system 00.02 – User authentication/authorization in SINS
		If the User successfully authenticates in SINS, proceed to step 3.
3	The user performs a search in the SINS to identify the signaling to which a flag is to be added	
		UC 11.01 – Complementary inquiry .
		If the signal to which you want to attach a flag has been identified, go to step 4, otherwise stop the current activity.
4	The user enters the data defining the flag in the form provided by the SINS WEB interface.	
5		SINS logs the request to add a flag to an existing flag.
6		SINS validates the request to create a flag addition to an existing flag according to the defined business rules.
7		If the request is valid, the use case continues from step 12, otherwise from step 8.

8		If the request to add a flag to an existing signal is invalid, SINS generates an error message in the WEB interface, in which the reason for the invalidation is explicitly indicated.
9		SINS logs the response to the request to add a flag to an existing flag (success, failure)
10	The user receives the error message and processes it.	
11		The use case is completed by the error message.
12		SINS creates the flag by entering all the information in the database.
13		SINS logs the operation of adding a flag to an existing flag
14		SINS makes the flag available for other operations.
15		SINS generates a confirmation message in the WEB interface. The confirmation message may also contain warning messages resulting from the verification of the business rules.
16		SINS logs the response to the request to add a flag to an existing flag.
17	The user receives the confirmation message from SINS.	

Post-conditions

- The flag is successfully created in SINS.
- The flag does not change the action to be followed in the SINS database
- The request to add a flag is sent to CS.SIS

Data provided by the user

- The country requesting the specification of an alternative action on its territory according to code_table ST001_RequestingUser
- The alternative action according to code_table ST105_ActionToBeTaken

screen

Screen – Add flag to a flag

At the end of the development phase of the project, the flag addition screen will be available. The screen will be built respecting the User Interface Specifications.

Associated Use Cases:

11.01 Complementary query

Following the Business Model:

Add flag to a flag

Other business processes triggered automatically:

N/A

1.1.2 USE CASE: 09 CHANGE FLAG ATTACHED TO A SIGNALING

Use Case ID: 10

Use case name: Change Flag attached to a signal

Range:

Use Case "**Modify Flag attached to a Signal", as part of the Use Case Diagram describes the general functionality of modifying a flag attached to a Romanian signal of Schengen interest.**

The flag applies only to the signals from Article 6 letter a and letter b, according to the legislation in force and to the signals related to discrete control.

Subsystem:

WEB	WAP	Message queues	WEB Services	FTP/SCP
YES	NOT	YES	NOT	NOT

Description:

The purpose of the Use Case is to modify an existing flag attached to an existing signal of Schengen interest belonging to the Romanian state.

Business Events:

The SIRENE Bureau of a member state requests the national SIRENE Bureau to modify a flag on a Schengen alert of interest belonging to the Romanian state.

Actors:

- The SIRENE Bureau through the SIRENE officer who has the right to modify a flag attached to an existing alert of Schengen interest belonging to the Romanian state
- Data provider system (national SIRENE Bureau system)

Prerequisites:

- The data provider system is operational
- The SINS system is operational
- The access interface to SINS is operational
- The user is authenticated in SINS and in the data provider system (National SIRENE Bureau System) and has the right to modify a flag attached to an existing alert
- The data provider system has all the necessary elements (at least the minimum mandatory information) for changing the flag
- The alert whose flag must be changed is an alert of Schengen interest, it has been sent to CS.SIS and there is a flag attached to it

Main Scenario –**Modification of the flag attached to an existing alert through message queues (in the case of the modernized IT system of the national SIRENE Bureau)**

Step	Data provider system (National SIRENE Bureau System)	MEANING
1	The data provider system authenticates.	
2		SINS verifies the authentication credentials and access rights related to the Data Provider System. UC 00.01 National System authentication in SINS.

		If the credentials of the provider System have been verified successfully, proceed to step 3.
3	The provider system generates the flag modification request attached to a signal and includes it in a message. The system places the message in its own output queue.	
4		SINS retrieves the message from the output queue of the Data Provider System.
5		SINS logs the flag modification request attached to an existing signal.
6		SINS checks the credentials of the user who requested the modification of the flag in the Provider System. UC 00.02 – User authentication/authorization in SINS
		If the User who requested the modification of the flag in the provider system successfully authenticates, then proceed to step 6.
6		SINS validates the structure of the received message by checking whether it complies with the validation scheme
7		If the message is valid the use case continues from step 14, otherwise from step 8.
8		SINS generates a confirmation message that explicitly indicates the reason for the invalidation.
9		SINS places the confirmation message in the input queue of the data provider System that sent the request.
10		SINS logs the confirmation of the flag modification request attached to an existing signal (successful, unsuccessful).

11	The provider system takes the confirmation message from its own input queue and processes it.	
12		The use case is completed by the error message.
13		SINS logs the confirmation of the flag modification request attached to an existing signal (successful, unsuccessful).
14		SINS validates the flag modification request attached to an existing signal according to the defined business rules.
15		If all business conditions are met the use case continues from step 21, otherwise from step 16.
16		If the request to change the flag attached to an existing signal sent through the message does not comply with the defined business rules, SINS generates a confirmation message that explicitly indicates the reasons for the invalidation and any warnings if any.
17		SINS places the error message in the input queue of the Data Provider System that submitted the request.
18		SINS logs the confirmation of the flag change request attached to an existing alert (successful, unsuccessful)
19	The provider system takes the confirmation message from its own input queue and processes it.	
20		The use case is completed by the confirmation message to the flag modification request attached to an existing signal (successful, unsuccessful).
21		The flag in SINS is changed by entering all the information in the database.

22		SINS logs the flag modification operation attached to an existing signal
2. 3		SINS makes the flag available for other operations.
24		SINS creates a confirmation message. The message may also contain warning messages resulting from the verification of business rules. SINS places the message in the input queue of the Data Provider System.
25		SINS logs the response to the flag change request attached to an existing flag.
26	The provider system takes the confirmation message from its own input queue and processes it.	

Alternative scenario –**Modification of the flag attached to an existing flag through the web interface**

Step	Delegated user of the Data Provider System (National SIRENE Bureau)	MEANING
1	The user logs in.	
2		SINS checks the credentials of the user who wants to connect to the UC system 00.02 – User authentication/authorization in SINS
		If the User successfully authenticates in SINS, proceed to step 3.
3	The user performs a search in SINS in order to identify the signal whose attached flag is to be changed	
		UC 11.01 – Complementary inquiry .
		If the signal to which you want to attach a flag has been identified, go to step 4, otherwise stop the current activity.

4	The user enters the data defining the flag in the form provided by the SINS WEB interface.	
5		SINS logs the flag modification request attached to an existing signal.
6		SINS validates the flag modification request attached to an existing signal according to the defined business rules.
7		If the request is valid, the use case continues from step 12, otherwise from step 8.
8		If the request to change the flag attached to an existing signal is invalid, SINS generates an error message in the WEB interface, in which the reason for the invalidation is explicitly indicated.
9		SINS logs the response to the flag change request attached to an existing flag (successful, unsuccessful)
10	The user receives the error message and processes it.	
11		The use case is completed by the error message.
12		SINS modifies the flag by entering all the information in the database.
13		SINS logs the flag modification operation attached to an existing signal
14		SINS makes the flag available for other operations.
15		SINS generates a confirmation message in the WEB interface. The confirmation message may also contain warning messages resulting from the verification of the business rules.

16		SINS logs the response to the flag change request attached to an existing flag.
17	The user receives the confirmation message from SINS.	

Post-conditions

- The flag is successfully modified in SINS.
- The request to change the flag attached to an existing signal is successfully sent to CS.SIS

Data provided by the user:

- The user can expand the list of countries that have requested an alternative action for a flag according to code_table ST001_RequestingUser
- The user can specify another alternative action according to code_table ST105_ActionToBeTaken

Screens:

Screen – Change flag

At the end of the project development phase, the flag modification screen will be available. The screen will be built respecting the User Interface Specifications.

Associated Use Cases:

11.01 Complementary query

Following the Business Model:

Change flag attached to an existing signal

Other business processes triggered automatically:

Notification

1.1.3 USE CASE: 11 DELETE FLAG ATTACHED TO A SIGNALING

Use Case ID: 10

Use case name: Delete Flag attached to a signal

Range:

Use Case "**Deleting a Flag attached to a Signal", as part of the high-level Use Case Diagram describes the general functionality of deleting a flag attached to a Romanian signal of Schengen interest.**

The flag applies only to the signals from Article 6 letter a and letter b according to the legislation in force and to the signals related to discrete control.

Subsystem:

WEB	WAP	Message queues	WEB Services	FTP/SCP	MEANING
YES	NOT	**YES**	**NOT**	**NOT**	**YES**

Description:

The purpose of the Use Case is to delete an existing flag attached to an existing signal of Schengen interest belonging to the Romanian state.

Business Events:

The SIRENE Bureau of a member state requests the national SIRENE Bureau to delete the flag attached to a Schengen alert of interest belonging to the Romanian state.

The signaling to which the flag was attached has been deleted from SINS

Actors:

- The SIRENE Bureau through the SIRENE officer who has the right to delete a flag attached to an existing alert of Schengen interest belonging to the Romanian state
- Data provider system (national SIRENE Bureau system)

Prerequisites:

- The data provider system is operational
- The SINS system is operational
- The access interface to SINS is operational
- The user is authenticated in SINS and in the data provider system (National SIRENE Bureau System) and has the right to delete a flag attached to an existing alert

- The data provider system has all the necessary elements (at least the minimum mandatory information) to delete the flag
- The alert has been deleted from SINS

Main Scenario –**Deleting the flag attached to an existing alert through message queues (in the case of the modernized IT system of the national SIRENE Bureau)**

Step	Data provider system (National SIRENE Bureau System)	MEANING
1	The data provider system authenticates.	
2		SINS verifies the authentication credentials and access rights related to the Data Provider System. UC 00.01 National System authentication in SINS.
		If the credentials of the provider System have been verified successfully, proceed to step 3.
3	The provider system generates the request to delete the flag attached to a signal and includes it in a message. The system places the message in its own output queue.	
4		SINS retrieves the message from the output queue of the Data Provider System.
5		SINS logs the request to delete the flag attached to an existing alert.
6		SINS checks the credentials of the user who requested the deletion of the flag in the Provider System. UC 00.02 – User authentication/authorization in SINS
		If the User who requested the deletion of the flag in the provider system successfully authenticates, then proceed to step 6.
6		SINS validates the structure of the received message by checking whether it complies with the validation scheme

7		If the message is valid the use case continues from step 14, otherwise from step 8.
8		SINS generates a confirmation message that explicitly indicates the reason for the invalidation.
9		SINS places the confirmation message in the input queue of the data provider System that sent the request.
10		SINS logs the confirmation of the flag deletion request attached to an existing alert (successful, unsuccessful).
11	The provider system takes the confirmation message from its own input queue and processes it.	
12		The use case is completed by the error message.
13		SINS logs the confirmation of the flag deletion request attached to an existing alert (successful, unsuccessful).
14		SINS validates the request to delete the flag attached to an existing signal according to the defined business rules.
15		If all business conditions are met the use case continues from step 21, otherwise from step 16.
16		If the request to delete the flag attached to an existing alert sent through the message does not comply with the defined business rules, SINS generates a confirmation message that explicitly indicates the reasons for the invalidation and any warnings if any.
17		SINS places the error message in the input queue of the Data Provider System that submitted the request.
18		SINS logs the confirmation of the flag deletion request attached to an existing alert (successful, unsuccessful)

19	The provider system takes the confirmation message from its own input queue and processes it.	
20		The use case is completed by the confirmation message to the request to delete the flag attached to an existing signal (successful, unsuccessful).
21		The flag in SINS is deleted by deleting all information from the database.
22		SINS logs the flag deletion operation attached to an existing flag
2. 3		MEANING: 1. archive the data related to the flag 2. update the signaling by deleting the attached flag
24		SINS creates a confirmation message. The message may also contain warning messages resulting from the verification of business rules. SINS places the message in the input queue of the Data Provider System.
25		SINS logs the response to the flag deletion request attached to an existing flag.
26	The provider system takes the confirmation message from its own input queue and processes it.	

Alternative scenario –**Delete flag attached to an existing flag through the web interface**

Step	Delegated user of the Data Provider System (National SIRENE Bureau)	MEANING
1	The user logs in.	
2		SINS checks the credentials of the user who wants to connect to the UC system 00.02 – User authentication/authorization in SINS

		If the User successfully authenticates in SINS, proceed to step 3.
3	The user performs a search in the SINS in order to identify the signal to which the attached flag is to be deleted	
		UC 11.01 – Complementary inquiry .
		If the signal for which it is desired to delete the attached flag has been identified, proceed to step 4, otherwise stop the current activity.
4	The user requests the deletion of the flag in the form provided by the WEB interface of SINS.	
5		SINS logs the request to delete the flag attached to an existing signal.
6		SINS validates the request to delete the flag attached to an existing signal according to the defined business rules.
7		If the request is valid, the use case continues from step 12, otherwise from step 8.
8		If the request to delete the flag attached to an existing signal is invalid, SINS generates an error message in the WEB interface, in which the reason for the invalidation is explicitly indicated.
9		SINS logs the response to the flag deletion request attached to an existing flag (successful, unsuccessful)
10	The user receives the error message and processes it.	
11		The use case is completed by the error message.
12		SINS deletes the flag by removing all information from the database.

13		SINS logs the flag modification operation attached to an existing signal
14		MEANING: 1. archive the data related to the flag 2. update the signaling by deleting the attached flag
15		SINS generates a confirmation message in the WEB interface. The confirmation message may also contain warning messages resulting from the verification of the business rules.
16		SINS logs the response to the flag deletion request attached to an existing flag.
17	The user receives the confirmation message from SINS.	

Post-conditions

- The flag is successfully deleted in SINS.
- The request to delete the flag attached to an existing alert is successfully sent to CS.SIS

Data provided by the user:

The operation to delete the flag attached to a signal

Screens:

Screen – Delete flag attached to a signal

At the end of the development phase of the project, the flag deletion screen attached to a flag will be available. The screen will be built respecting the User Interface Specifications.

Associated Use Cases:

11.01 Complementary query

Following the Business Model:

Delete flag attached to a signal

3. Flagging methods to be implemented; method description

CreateFlag

Description	Operation by which the SIRENE Bureau adds flags requested by other member states to the alerts introduced by the Romanian state.
SINS operation called	CreateFlag
Input	alert [SchengenId] – the Schengen identifier of the alert to which the flag belongs. flag [Flag] – the flag to be created; context [Context] ; [Context]=(User, role, institution) **<u>Explanations</u>** the flag record is created in the tables: T_FLAGGING_VF ([VF_ID], [AL_ALERT_NB], [ST001_ID], [ST105_ID], [VF_CSURN], [VF_OPERATION]); T_FLAGGING_VF = 'The table contains the data of the flag, which can be attached to an alert.'; T_FLAGGING_VF.VF_ID = 'This attribute contains the ID of the Flag'; **compulsory** T_FLAGGING_VF.AL_ALERT_NB = SchengenID of the flagged alert;); in this field the calculated value of SchengenID is written using the elements: (SNCreateFlag.Request.SchengenID.RequestingUser, SNCreateFlag.Request.SchengenID.NationalNumber.IDNumber, SNCreateFlag.Request.SchengenID.NationalNumber.RecordType) from the SNCreateFlag.xsd scheme as parameters in the function calculatedSchengenID; mandatory T_FLAGGING_VF.ST001_ID = FK(ST001.ST001_ID); example: ST001. ST001_ID = "0025.01", associated with column ST001.ST_CODE = "0025"(Slovakia); in this field write the value of the element SNCreateFlag.Request.SchengenID.RequestingUser from the scheme SNCreateFlag.xsd.; optional T_FLAGGING_VF.ST105_ID = FK(ST001.ST005_ID); example: ST005. ST005_ID = "0004.01"; in this field write the value of the SNCreateFlag.Request.Flag.AlternativeActionToBeTaken element from the SNCreateFlag.xsd scheme; optional T_FLAGGING_VF.VF_CSURN = 'Update Request Number of the last CUD'; to be identified; the previously calculated SchengenID field is used to identify the corresponding alert in T_ALERT_AL, from which the

	T_ALERT_AL.AL_CSURN field associated with the respective alert is extracted; mandatory **Q1D(open):**is the field T_ALERT_AL.AL_CSURN (SchengenID) associated with the flagged alert used, or is it T_ALERT_AL.AL_CSURN taken from the last existing record in the table? T_FLAGGING_VF.VF_OPERATION = 'This attribute contains the operation used on the alert C(Create), U(update), D(delete); NOTE:in this field, the value of the SNCreateFlag.Header.Operation element from the SNCreateFlag.xsd scheme should be written, i.e. related to ST209.ST209_ID. However, what is required is only a literal identification of the performed operation, i.e. only 'C', 'D', 'U' is written, the writing space allocated being 1 byte in the referred table; compulsory For writing, the "Flag" entity class is used <class>Flag <attribute set>RequestingUser, NationalIDNumber, RecordTip, RequestingCountry, AlternativeActionToBeTaken, <class>Alert</class> , <class>User</class></attribute set> </class>
Output	code [ReturnCode]-the SINSCreateFlag object is returned, incorporating the RCI/atrib object. ReturnCode
Error messages	error [ErrorCode] – Error code; the SINSCreateFlag object is returned, incorporating the RCI/atrib object. ErrorCodes

UpdateFlag

Description	The national system requests the updating of an existing flag
SINS operation called	UpdateFlag
Input	alert [SchengenId] – the Schengen identifier of the alert to which the flag belongs. flag [Flag] – the updated flag. context [Context] - User, role, institution.
Output	code [ReturnCode]
Error messages	error [ErrorCode] – Error code

DeleteFlag

Description	The national system requests the deletion of an existing flag from the system.
SINS operation called	DeleteFlag
Input	alert [SchengenId] – the Schengen identifier of the alert to which the flag belongs.

	context [Context] - User, role, institution.
Output	code [ReturnCode]
Error messages	error [ErrorCode] – Error code

4. Planning

Discipline	**Task**	**Artifacts**	**Role**
Architecture	Definition of Work Order	Work Order	SW Architect
Project Management	Planning	Project Plan	Project Manager
Architecture	Definition of signatures with IN, OUT parameters and associated Error codes.	List of signatures, input, output parameters	SW Architect
System Microdesign	Class Diagram	Class Diagram	SW Architect
System Microdesign	Interaction Diagram (Sequence Diagram)	Interaction Diagram	SW Architect
Development	Method 1: CreateFlag	EJB	Programmer
Development	Method 2: UpdateFlag	EJB	Programmer
Development	Method 3: DeleteFlag	EJB	Programmer
Development	Method 4	EJB	Programmer
Development	Build and test	EARLY	Programmer
Quality Assurance	tESTING	Test Report	QA Consultant