1.2.1. USE CASE: 01. CREATE SIGNALING

Use case ID: 01

Use case name: Create Signaling

Range:

The high-level Use Case "Create Alert" describes the general functionality of adding an alert, common to all types of alerts. The particularities for each type of signaling are detailed in the specific use cases for each type.

Subsystem:

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

Description:

The purpose of the Use Case is to create a new signal in SINS, as a result of its creation in the external system of the data supplying authority, in accordance with the SCHENGEN regulations and the national legislation in force.

Business Events:

Creating a flag in the source provider system.

The user or an external system requests the creation of signaling through the SINS access interfaces.

Actors:

- Data provider system (external national system)
- Users with the role of entering, modifying and deleting alerts

Prerequisites:

- The notification is of interest to SINS (whatever its type: National or Schengen)
- 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 national data provider system and has the right to create a report
- The data provider system has all the necessary elements (at least the minimum mandatory information) to create a signal
- The provider system provided the value of the multipleCheck boolean parameter (TRUE - indicates whether, following the creation of the alert and the verification of multiplicity and incompatibility, SINS will populate the lists of alerts related to cases of multiplicity and incompatibility or FALSE - SINS will not populate the lists of multiple or incompatible alerts) . Regardless of the setting of the flag, the multiplicity and incompatibility checks are always performed, the flag only altering the content of the response.
- The data provider system provided the value of the boolean parameter ISForcedDuplicates (TRUE – the creation of the notification in SINS will be forced at the sole responsibility of the national authorities, even if it is in a possible case of duplication or FALSE – the notification will not be created in SINS, this being in a possible case of duplication). Regardless of the setting of the flag, checks for duplicate alerts are always performed, even if the user decided to force the creation of the alert in SINS. The response to the check for duplicate alerts will be received by the user together with the list of multiple and incompatible alerts.

Main Scenario - Creation of signaling through message queues (in the case of Modernized National Systems)

Step	Data provider 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 signal creation request 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 signal creation request.
6		SINS checks the credentials of the user who created the alert in the Provider System. UC 00.02 – User authentication/authorization in SINS
		If the User who created the alert 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 signal creation request (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 signal creation request (successful, unsuccessful).
14		When requesting to create a SINS alert, it checks the following:
		14.1.SINS validates the request to create a signal according to the business rules defined for each type of signal separately (see Annex III). If at least one business rule is not met, SINS generates an error message.
		14.2 After checking the business rules, SINS checks if the signal that is to be created is in conflict with another signal (multiple or incompatible) or duplicate. The conflict detection check is carried out by running the query 11.03 Query for multiple and incompatible signals. The duplicate check is carried out by comparing the fields that are the subject of checks for each type of signaling in part as they were parameterized by the SINS Central

		Administrator, through the business rules administration functionalities made available by the system.
15		If all the business conditions are met and the check for duplicate alerts was successful or it was requested to force the creation of the alert in SINS, the use case continues from step 21, otherwise from step 16.
16		If the signaling transmitted through the message does not comply with the defined business rules or the signaling is found to be duplicated and it was not requested to force its creation, SINS generates a confirmation message in which the reasons for the invalidation are explicitly indicated. The confirmation message may also contain explicit markings highlighting cases of duplicate alerts. (Schengen ID is not generated, the signal creation UC stops).
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 signal creation request (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 signal creation request (successful, unsuccessful).
21		SINS creates the notification in SINS by entering all the information in the database and the Schengen ID is generated.

22		SINS logs the signal creation operation.
2. 3		SINS makes signaling available for other operations.
24		The use case is completed by the confirmation message to the signal creation request (successful). The confirmation message also contains the list of alerts with which the newly created alert is in conflict (multiple or incompatible) or duplicate.
25	The provider system takes the confirmation message from its own input queue and processes it.	

Alternative scenario - Creating signaling through the Web interface

Step	Delegated user of the data provider System	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 enters the data defining the new signaling in the form provided by the SINS WEB interface.	
4		SINS logs the signal creation request.
5		When requesting to create a SINS alert, it checks the following:
5		**5.1.**SINS validates the request to create a signal according to the business rules defined for each type of signal separately (see Annex III). If at least one business rule is not met, SINS generates an error message.
		5.2 After checking the business rules, SINS checks if the signal that is to be created is in conflict with another

		signal (multiple or incompatible) or duplicate. The conflict detection check is carried out by running the query 11.03 Query for multiple and incompatible signals. The duplicate check is carried out by comparing the fields that are the subject of checks for each type of signaling in part as they were parameterized by the SINS Central Administrator, through the business rules administration functionalities made available by the system.
6		If the request is valid, the use case continues from step 11, otherwise from step 7.
7		If the request to create a signal does not comply with the defined business rules or the signal is found to be duplicated and it was not requested to force its creation, SINS generates a confirmation message in which the reasons for the invalidation are explicitly indicated. The confirmation message may also contain explicit markings highlighting cases of duplicate alerts. (Schengen ID is not generated, the signal creation UC stops).
8		SINS logs the response to the signal creation request (successful, unsuccessful)
9	The user receives the error message and processes it.	
10		The use case is completed by the error message.
11		SINS creates the alert by entering all the information in the database and the Schengen ID is generated.
12		SINS logs the signal creation operation.
13		SINS makes signaling available for other operations

14		The use case is completed by the confirmation message displayed in the WEB interface upon the signal creation request (successful). The confirmation message also contains the list of alerts with which the newly created alert is in conflict (multiple or incompatible) or duplicate.
15	The user views the confirmation message from SINS.	

Alternative scenario - Create signaling by exchanging files via FTP

Step	Data provider system	MEANING
1	The provider system generates a file containing the alerts that must be created.	
2	The provider system places the file in its private directory on the FTP server of SINS respecting the predefined security rules.	
3		At well-established times, SINS checks the availability of files on the FTP server.
4		SINS retrieves the files from the FTP server
5		SINS logs the operation of retrieving files from the FTP server.
6		SINS checks if the Data Provider System authenticates.
		SINS verifies the authentication credentials and access rights related to the Data Provider System. **UC 00.01 National System authentication in SINS.**
		If the provider System authenticates, proceed to step 7.
7	SINS checks the structure of the received file	
8		SINS validates the structure of the received file.

9		If the file has a valid structure, the use case continues from step 16, otherwise from step 10.
10		If the file has an invalid structure, SINS creates a log and error (response) file that will contain the error message.
11		SINS logs the failed file processing attempt in the FTP log.
12		SINS notifies authorized users of the Data Provider System that submitted the file about the availability of the log and error file.
13	Users are notified about the availability of the log file and errors on FTP. The file is downloaded from FTP for processing.	
14		The use case is completed by an error recorded in the log file and errors.
15		SINS logs user notification activity regarding the availability of the log file and errors on the FTP server.
16		For each signal in the received file, SINS executes steps 16.1 - 16.9:
16.1		SINS validates the signaling according to the business rules for each type of signaling.
16.2		SINS validates the request to create a signal according to the business rules defined for each type of signal separately (see Annex III). If at least one business rule is not met, SINS generates an error message.
16.3		After checking the business rules, SINS checks if the signal that is to be created is in conflict with another signal (multiple or incompatible) or duplicate. The conflict detection check is carried out by running the query

		11.03 Query for multiple and incompatible signals. The duplicate check is carried out by comparing the fields that are the subject of checks for each type of signaling in part as they were parameterized by the SINS Central Administrator, through the business rules administration functionalities made available by the system.
16.4		SINS logs the signal creation operation.
16.5		SINS logs the signal creation operation, in the log related to FTP operations.
16.6		SINS makes signaling available for other operations.
16.7		SINS fills in the log file and errors the created signaling and the warning messages resulting from the verification of the business rules, including the verification of multiplicity-compatibility or multiplicity incompatibility with the highlighting of duplicate cases; the use case continues from step 16.1 until all signatures received in the FTP file are completed.
16.8		If the data related to the signaling is incomplete or invalid, SINS stores the invalid signaling in an intermediate database (Staging database). In this case, the multiplicity-compatibility or multiplicity-incompatibility check is not performed, as the Schengen ID is not generated.
16.9		SINS fills in the log file and errors, for each individual signal.
17		SINS notifies authorized users of the Data Provider System regarding the completion of file

		processing and the availability of the log and error file.
18	Users are notified about the availability of the log file and errors on FTP. The file is downloaded from FTP for processing.	
19		SINS logs the operation to notify users about the availability of the log file and errors.
20	The user logs in to the WEB interface of SINS.	
21		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 logs into SINS, go to step 22.
22	The user identifies the alert he wants to create by filling in invalid or missing data.	
2. 3		Query signaling in the Staging Database.
24	The user fills in the missing data and/or modifies the invalid data of a signal saved in the intermediate database (Staging database) through the form provided by the SINS WEB interface. UC 19. Completion of signal data received SN	
25	The use case continues with step 4 of the alternative scenario of the Create Web Signaling use case.	
		The signaling is created and the Schegen ID is generated.

Post-conditions

- The alert is successfully created in SINS, the duplicate, multiplicity and incompatibility checks were successful, the schengen ID is generated.
- Depending on the values of the multiplecheck boolean parameter, following the checks of multiple and incompatible alerts, SINS will send the national authority

the response regarding the creation of the alert, including the lists with which the created alert is in a possible conflict (multiplicity and incompatibility)

- If the national authority forced the creation of a duplicate alert in SINS, it will generate the lists of multiple and incompatible alerts with the highlighting of duplicate cases.
- If SINS, upon the request to create a signal, has identified a duplicate case and the ISForcedDuplicates parameter is set to FALSE, it will reject the creation of the signal.
- If the request to create a signal is rejected, SINS will generate corresponding messages
- When creating the signaling in SINS, its initial status indicators are set as follows: isNationalValid=true; isSchengenValid=false; isSchengenExported=false
- Status indicators will change, according to business process 01. Create signal
- Only after the settings of the above parameters take place, the signaling becomes visible in SINS and available for any other operations performed by authenticated users (modification, addition to a link, query, etc.).
- SINS sends a notification creation confirmation to the user delegated by the Data Provider System (the notification creation confirmation also contains the results of checks for multiple and incompatible notifications and, as appropriate, the marking of cases of duplicate notifications)
- The log and error files received by the non-modernized national authorities, after processing, will contain either error messages or confirmation messages as a result of the creation of alerts in SINS.
- SINS sends a notification about the creation of an alert to users who have subscribed to notifications by event type.

Data provided by the user:

Cf attributes specific to each type of signaling in part described in Annex III to the Use Case Model document, for each entity and type of signaling in part.

screen

SCREEN – Create signaling

At the end of the development phase of the project, a screen will be available for each type of signaling. The screens will be built respecting the User Interface Specifications.

Associated Use Cases:

00.01. National System authentication

00.02. User authentication/authorization

19. Completion of received SN signaling data

Other Use cases triggered automatically

11.03 Query execution for multiple and incompatible signals

Following the Business Model:

Signal Creation Process

Other Businesss processes triggered:

User notification