COUNCIL OF THE EUROPEAN UNION

Brussels, 28 May 2014 (OR. en)

10303/14

DAPIX 72
ENFOPOL 147
SIRIS 41

NOTE

From:	German delegation
To:	Working Group on Information Exchange and Data Protection (DAPIX)
Subject:	HENU Workshop on SIENA Implementation - Roadmap on SIENA implementation

1. Introduction

In the Stockholm Programme prepared in July 2009, the Council requests the European Commission *inter alia* to study the exchange of information of the law enforcement authorities and the creation of a European information exchange model[1]. The European Commission initially responded by preparing an overview of the instruments used in the EU for multilateral exchange of experience with crime fighting[2] and, on the basis of this overview, it presented the „European Information Exchange Model“ (EIXM) in December 2012[3].

1 Cf. European Council, 2010, pp. 17 ff.
2 Cf. European Commission, KOM(2010) 385.
3 Cf. European Commission, KOM(2012) 735.

The Swedish Initiative, the Prüm Council Decision, Europol and SIS are emphasised as essential instruments of the EIXM, with the SIRENE-Network, the Europol channel and the Interpol channel being presented as essential communication channels.

In the process, the European Commission also clearly states that the selection of communication channels is largely made on the responsibility of the individual Member States and is only dealt with and governed to a minor extent by European law.[4] Many states welcome the absence of a stipulation regarding an information channel to be used as a matter of principle and prefer being able to select the scope of co-operation based on the merits of each individual case.[5]

However, this flexible use of communications channels is not considered expedient by the European Commission. The latter perceives the necessity of an improved structuring of the exchange of information and encourages the member states to use the Europol channel as the default channel unless some other communications channel is stipulated in legal terms. In the process, the Commission emphasizes various advantages of the Europol channel, including the special facilities of the interoperable communication platform Secure Information Exchange Network Application (SIENA) and the national liaison officers deployed at Europol.[6]

In the light of these developments a discussion was launched at the HENUs meeting on 30 October 2013, in particular regarding following questions:

4 For instance, inquiries regarding investigation matters in the Schengen information system need to be made via the national SIRENE offices; cf. European Commission, KOM(2012) 735, p. 7.

5 The study published in June 2012 and the explanatory notes of RAND Europe on the evaluation of Europol indicate that this interpretation is confirmed ("an obligation would risk damaging trust relationships with Member States"), cf. *Disley/Irving/Hughes/Patruni*, 2012, p. 56 f.

6 Cf. European Commission, KOM(2012) 735, p. 10.

What can Member States and Europol do in order to optimize the implementation and extend the use of SIENA at national level ?

Can Member States identify common ground for activities and developments ?

The HENU group decided to set up a HENU SIENA workshop regarding the Member States' (MS) and Third States' (TP) activities to implement SIENA in their national workflow. Participants of the first workshop, which took place on 21 November 2013, were representatives of the Liaison Bureaux and Europol; one country was also represented by the Europol national Unit (ENU).
The participants of the workshop merged their professional experiences in a brainstorming session without representing the formal posture of their respective country. As an outcome of this workshop the participants decided to draft a roadmap on SIENA implementation including possible actions to be undertaken by MS, TP and Europol. This roadmap entails recommendations to the HENUs on how to implement SIENA in a most effective way at national level. The roadmap can be used as a guidance to help the ENU and Europol Liaison Bureaux (ELB) in advising the relevant stakeholders in their countries, including the Management Board and the Council DAPIX Working Party.

2. Goals and concrete actions to be undertaken:

The implementation of the proposed goals and recommended actions is subject to the national legislation and working procedures of the respective Country.

2.1. Promote and define the Europol channel as the channel for international law enforcement cooperation at European level

Concrete recommended actions:

- **Create a Single Point of Contact (SPOC) in the MS and TP where operators are able to use all communication channels including the 24/7 availability and handling of SIENA**

- **Enhance awareness regarding the different ways of using SIENA**

  The document “SIENA DOs and DON’Ts and SIENA Glossary” (EDOC#714996v1) regarding the different ways of using SIENA has been updated and can be used in this process.

  Europol will launch the EPE platform on SIENA, EIS and IAM for Member States and Third Parties to share experiences amongst each other.

- **Intensifying SIENA training at national level**

  For most MS it is still a big challenge to make the law enforcement authorities aware of the possibilities of the Europol channel. An increase of trained staff at national level might help to overcome these obstacles. This would also reduce the number of operator errors.

- **Provide a common exchange programme for SIENA operators on a European wide scale**

  Explore the possibilities to implement a similar approach as adopted by the SIRENE Group, where SIENA operators can undertake exchange study visits to facilitate familiarisation with European information exchange practises.

  Look into different ways of financing this initiative (e.g. EU funding from various sources). Invite CEPOL to assess the integration of this topic into their annual exchange programme planning.

- **Enhance decentralised use of SIENA at national level**

  One of the advantages of SIENA is the ability to communicate directly from one Designated Competent Authority (DCA) to another in a secure environment. The decentralised use of SIENA will affect the existing national business processes and should therefore be handled by means of a step by step approach. Appropriate training and awareness is a prerequisite to meet the highest possible quality standards.

- **Provide a multilingual SIENA interface by Europol**

  The multilingual SIENA interface will enable the operators at ENU and decentralised level to display SIENA in their own national language.

- **Provide an automated translation of free text fields in SIENA messages by Europol**

  The automated translation of free text in SIENA messages will give the investigator a first idea of the content of the data exchange. This aid will be based on the SYSTRAN technology.

- **Set-up a web service**

  As from end 2012, it is possible to create an interface to connect national case management system(s) with SIENA. This facilitates the automated data exchange processes whereas the incoming and outgoing data can be recorded automatically. The first interface has already been developed in Germany. At the SIENA product management meeting in December 2013 other Member States expressed their interest to start the development of a similar web service SIENA interface[7].

- **Proper use of EU-funding**

  The EU-funding is essential to overcome the national constraints and to speed up the process of SIENA implementation at national level. EU funding can be used e.g. to upgrade the national secure lines in order to meet the security and accreditation level of SIENA, to set-up the web service to connect the national case management system to SIENA, as well as for training and awareness purposes such as the exchange programmes of SIENA operators.

  Continue the dialogue with the European Commission on the EU funding possibilities.

[7] Further detailed information on the web service can be retrieved in the annex on SIENA integration with national systems attached to this note.

- **Remote SIENA access**

  Europol should promote the remote SIENA access (e.g. laptops, mobile devices) for Member States and Third Parties.

  Europol should assess the possibilities to receive a notification message on the remote device.

2.2. Enrichment of crime analysis and fasten the data processing at Europol

The data import in the new Europol Analysis System can be automated by means of structured data exchange in SIENA. This automated data import will speed up the data processing at Europol whereas Member States and Third Parties will benefit from a fast cross check response from Europol. The use of structured data exchange will not only speed up the data processing, it will also enhance the quality of the data exchanged and reduce translation efforts. Ultimately this would lead as well to a larger data volume, potentially resulting in a higher number of hits.

Concrete recommended actions:

- **Implementation of UMF structured data in SIENA by Europol**

  The implementation of the UMF structured data format in SIENA should be intensified. The structured data will support the automated cross-check of the data with the Europol databases.

- **Use of the UMF structured data in SIENA by MS and TP**

  In order for the data processing such as cross-check performance to be automated and speeded-up, Member States and Third Parties need to use the structured data fields in the SIENA message. This can be done manually, by typing the data in the structured data fields, or automatically by means of the web service.

2.3. Enhance the cross check of information by the Operational Centre

In order to guarantee a swift response to cross-check requests and for Europol to fully support the Member States in providing cross match analysis at any time, the Europol Operational Centre should be available, monitoring and handling SIENA messages on a 24/7 basis.

Concrete recommended actions:

- **24/7 availability and handling of SIENA at Europol**
- **Implementation of UMF structured data in SIENA by Europol**
- **Use of the UMF structured data in SIENA by MS and TP**

2.4. Common understanding of the use of SIENA for the law enforcement data exchange

SIENA implemented the requirements of the Swedish Initiative data exchange and supports the Prüm hit follow-up in accordance with the Prüm Council Decision. The elimination of SISNET could lead to a possible shift to the Europol channel to exchange data in accordance with the Schengen Agreement.

Concrete recommended actions:

- **Use of SIENA for Prüm hit follow-up data exchange**

  We currently face the situation that the communication channel used to exchange Prüm hit follow-up data varies from country to country.

- **Use of SIENA for Swedish Initiative requests and replies**

  SIENA supports the information exchange in accordance with the Swedish initiative. SIENA entails Swedish Initiative specific forms including all mandatory fields according the council framework decision 2006/960/JHA. The use of the Swedish-Initiative had not yet reached its full potential; therefore, using the user friendly Swedish Initiative form in SIENA could promote the use of this legal instrument.

- **Use of SIENA for the information exchange that was formerly handled via SISNET**

  With the implementation of SIS II communication network, the former SISNET data exchange has been disabled. The SIS II communication network is legally limited to SIS II data and supplementary information. Therefore, the information exchange according to art. 39 and art. 40 Schengen convention, which was formerly done via SISNET, has to be handled via another communication tool.

2.5. Enrich the information exchange with Europol in counter terrorism cases

At present the majority of counter terrorism data exchange is dealt with via the PWGT. This PWGT communication tool needs to be replaced in order to further support this type of data exchange. SIENA can be considered as a future option of the communication tool currently used by the PWGT, to safeguard the data exchange on counter terrorism. The use of SIENA as communication tool would enable MS and TP to make use of the services and products provided by Europol more often by using one means of communication. The PWGT could benefit from the support delivered by the Europol such as operational and strategic crime analysis and data cross-check as well as from the added value of the Liaison Bureaux network.

Concrete recommended actions:

- **Assess the feasibility to use SIENA for the information exchange of the Police Working Group on Terrorism (PWGT)**

  Inform the PWGT about the possibilities of SIENA. The PWGT could be a closed SIENA user group in order to limit the access to this data exchange to the authorized persons.

- **Upgrade the confidentiality level of SIENA to EU Confidential**

  In order to enable the use of SIENA by the PWGT, Europol should analyse the EU Confidential confidentiality level for SIENA.

2.6. Strengthen the role of the Liaison Officers at Europol

Many ELO spend the bulk of their service time in translating and managing SIENA messages. The potential of the ELO set up at Europol should be better exploited to further improve the quality and speed of multilateral exchange of information. Consequently, the world wide unique cooperation of the ELBx and Europol should be intensified. The differences relating to the legal regulations of the individual Member States but also the socio-cultural aspects should be handled more effectively.

Concrete recommended actions:

- Dual use of SIENA via
  - Set-up of web service
  - Decentralised use of SIENA

  The LBx at Europol do not necessarily need to be engaged in the so-called mass correspondence in SIENA where messages can be prepared, dispatched and received via SIENA on a central basis (SPOC) as is the case for the Interpol channel. The ELO and the analysis capacities of Europol should be more used for complex investigations calling for specific coordination efforts.

  Accordingly, a dual Europol channel can be created that entails on the one hand the exchange of information between the ENUs and, on the other hand the engagement of the ELO and special support capabilities of Europol. In those cases falling within the Europol mandate, the 24/7 Operational Centre should be engaged in order to obtain a cross-check with the data available in the Europol databases.

2.7. Description of business processes at national and international level

In addition to creating the technical prerequisites, the business processes in the Member States and Third Parties also need to be elaborated and described. It has to be specified at national level who is responsible for which action e.g. who translates the SIENA messages, who ensures the quality checks, and so on. Further more, a Service Level Agreement between the Member States, Third Parties and Europol should be set up, which could be based on the SIENA DOs and DON'Ts document.

ANNEX

SIENA Integration with National Systems

Purpose

This document aims to serve as a starting point for Member States and Third Parties with which Europol has an operational agreement that are considering to make use of the possibility to integrate a national system with SIENA.

Introduction

SIENA is Europol's secure information exchange system. It allows Law Enforcement officers to exchange information using a web browser. The ability to access SIENA using a web browser (Internet Explorer or Firefox) is the primary interface and it is offered to all SIENA participants.

SIENA however also facilitates *system to system* connection, enabling systems (instead of people) to exchange information through SIENA. This functionality has been released at the end of 2012. It was tested with Germany and found to be fully operational. It is currently in use by Germany, but is now available for all Member States as well as operational Third Parties. Note that when a country chooses to use this system to system connection the primary interface, allowing users to connect with a web browser, remains available as is.

Two types of system to system connection are facilitated; simple and advanced.

Simple

The simplest way to interact with SIENA is to connect a national system only for receiving SIENA messages. Messages will not be sent by the national system through SIENA. The system will only receive:

- All messages received by your country. Here it does not matter if a competent authority receives the message or the LB/ENU/NCP; all messages will be provided to the national system
- All messages sent by your country using the primary interface (a user using a web browser).

This can be convenient for registering all messages exchanged in SIENA where your country is involved. One does not need to implement the complex SIENA logic describing when a message is pending sent, pending received, handled, unhandled, etcetera. It is however likely that custom software development work will be required, which needs to be executed under national responsibility.

Advanced

The more advanced way to interact with SIENA is to connect a national system both for sending as well as receiving messages. So here messages can not only be received by the national system, but also sent. This has the possibilities as described above for the simple connection, as well as:

- The ability to send SIENA messages

This allows Law Enforcement officers using the national system to exchange SIENA messages with their international counterparts. These users never have to access SIENA, yet are still able to use the SIENA channel. This can have many advantages, such as:

- Law Enforcement officers can use *one* system for both their national cases as well as their international cases.

- SIENA needs to facilitate many Member States and cooperation partners. Your national system can be tailor made to match perfectly the national circumstances and legislation. Therefore using your national system might be more convenient for Law Enforcement officers.

- In case the national system also has a connection to other channels (e.g. the Interpol channel), as is the case for the German system, the choice of channels is simplified since all information can be handled in a similar way.

Note that the advantage that your national system has a user interface in your national language is not mentioned here above, as the current plans foresee that the SIENA user interface is made multilingual in the course of 2014.

The ability to send messages needs to be accompanied in your national system with a correct implementation of the SIENA logic describing for example when a message is pending sent or pending received, handled or unhandled, when a cancellation can be sent etcetera. It is likely that custom software development work will be required, which needs to be executed under national responsibility.

Technical specification

The national system interface is designed as a *web services interface* combined with an *FTP service* to exchange attachments. The national system needs to poll SIENA on a regular basis to check if new messages are available. The interface is providing only *message exchange* functionality to enable exchange with other countries or organisations. Functionality like drafting, internal communication or assignment, tasking, marking a message as in progress, search and statistics is excluded. Your national system would need to provide for this functionality as required.

Europol provides an online test environment in order to enable Member States and operational Third Parties to test their systems using strictly non-operational test data. Periodic re-testing (regression testing) will be required when Europol is releasing a new version of SIENA, in order to ensure that future versions of SIENA will still work correctly with your national system. Europol will strive to maintain the interface specification for a period of time still to be defined. After this period you can be required to upgrade your interface with SIENA in order to support new functionality. An example could be the creation of a new messages type. The following changes are foreseen for the near future:

- Ability by the national system to content delete a message
- Ability by the national system, when sending a message, to set the sending unit (LB/ENU/Competent Authority). Currently all messages sent by the national system through SIENA as specified as coming from the ENU.
- Ability by the national system to set the case name and to retrieve the case name on every message.
- Ability to exchange structured data according to the UMF2 format

SIENA supports *only one national system* per country. It is possible that this will change in the future, however for now this does not seem likely due to resource constraints. In case you would like *multiple* national systems within your country to connect to SIENA, you would have to create a system in between those systems that can route the incoming messages to your different national systems as required, and that routes outgoing messages from the different national systems to SIENA.

How to proceed

Member States and operational Third Parties are invited to connect a national system to SIENA. Please contact Europol if you wish to do so. Europol will then provide you with assistance, including the most recent technical interface definition, in order to support you to initiate the adjustment of your system.

Annex: Formal interface requirements

For further reference the formal requirements for the national systems interface are described is this chapter.

Definitions

OE: Organisational Entity; this represents a country or a Europol unit, an AWF, or a Eurojust National Member.

OSE: Organisational Sub Entity; this represents the Liaison bureau, National Unit, National Contact Point, or other competent authority, or a part or a group of these. It can represent a Focal Point or a Europol sub-unit.

Functional

The following functionality is provided by the SIENA interface to National Systems.

1. Sending a message to another OE.

    a) The message can contain one or more attachments.

    b) The receiving end can use the SIENA web interface, their national system (if connected), or both

    c) The send message is also visible in the OE of the sender (under *Sent* and/or *Pending sent*)

2. Receiving a message from another OE.

    a) The message can contain one or more attachments.

    b) The received message can be received both in the SIENA web interface as well as the national system.

    c) A received message is provided once to the national system. After that it is marked as read by the national system.

3. Providing a list of recipients (OEs and OSEs)

    a) Because some OSEs cannot send to some locations, this list can differ depending on for which OSE this list is requested.

    b) The full list of recipients (independent of whether the recipient can be sent to) can also be retrieved.

4. Receiving a copy of a message send by your own OE through the SIENA application (web interface)

    a) Whenever someone uses the Web Application to send a message, the National System must receive the message as well. This will make sure that the pending sent / pending received status can be maintained correctly, and that both in the Web Application as well as in the National System a complete picture of all information can be maintained.

5. A message will be provided by SIENA to the National System in a structured way.

    a) An XML structure must be used.

    b) Both normal messages as well as messages according to the Swedish Initiative must be supported.

    c) The functional structure of the message must be identical on the Web Application and the Web Service.

    d) A SIENA message number is provided upon sending or receiving a message.

    e) In case a received message is related to another message, the SIENA message number of the related message is also provided.

    f) The National System can provide an identifier for the message using the “National Message ID” field

The following functionality is excluded. If required, this needs to be covered in the national system.

6. Creating a draft message

7. Searching for messages

8. Assigning or tasking messages

9. Internal communication

10. Accessing statistics

11. Receiving old messages (possibly in the future)

Other constraints

12. Only one National System can be connected to SIENA per OE.

13. SIENA has no notion of *users* inside the national system. The national system is regarded as one entity with respect to security and assignment.

14. There is no case based access (limitation of message accessibility depending on OSE) enforced to the national system.

15. It is possible for the national system to determine for a received message to which OSE the message was sent. It is not possible to determine if this message was assigned to another OSE using the SIENA web interface.

16. It is possible for a Member State to use both the Web Application as well as the National System.

17. Actions taken in the Web Application (e.g. assignment, translation, drafting, sending) will not be visible using the interface with National Systems.

18. A message send using the interface with National Systems will be visible as a (pending) sent message in the Web Application.

19. The interface that is provided to the National System is a temporary interface. The final interface will be created at a later stage. This more mature interface is likely to build upon the work done in the UMF2 project.

20. A message can be retrieved only once by the National System. Once a message is retrieved successfully, it will not be provided to the National System again (e.g. a stack from which items are “popped”).

The following functionality is provided by the National System.

21. As a minimum the status of Pending Received is maintained correctly, in order for users in the National System to be able to know when they are expected to reply to a message.

22. Preferably the status of Pending Sent is maintained correctly, in order for users in the National System to be able to know when they can still expect a reply.

23. The National System acts as one OSE, for example the ENU or a newly to be defined OSE.

    a) In SIENA this OSE has property “Default access” set to “True”.

    b) It will not be possible for the National System to assume the identity of another OSE to be able to address a message to different participants.

Technical

24. National case management system of the country must be connected to the SIENA Web Service.

25. The SIENA Web Service is a passive system.

26. The SIENA Web Service must allow to send a message from a National System to more than one recipient concurrently

27. The SIENA Web Service must only provide messages sent to the OE of the country. Messages which are not sent to the specific OE must be invisible.

28. It must be possible to send and receive attachments in a message. This will work by uploading (send) or downloading (retrieve) files on a fileshare.

29. The National System of a country must authenticate itself to the SIENA Web Service.

30. The SIENA web service must be described in a WSDL with XSD. This must be provided by Europol to the country.

Non-functional

31. Reliability: reliability of the exchange is considered critically, i.e. a high assurance should be provided that messages are not dropped, duplicated or modified.

32. Scalability and performance: for now the solution may have scalability constraints, particularly in terms of message throughput. The solution may impose limitations in the volume of messages that can be exchanged, the performance of the exchange and the response times as the volume of messages increases.

33. Architecture compliance: the solution will be based on open standards and aligned with the overall Europol ICT architecture.

34. Changeability and maintainability: the solution architecture will be designed modularly, with open interfaces between components, enabling separation of concerns and facilitating changes.

35. Testability: the development and testing environments of both Europol and the national system should enable integration testing of the solution prior to deployment in production.

Security requirements & considerations

The integration of SIENA with the national system will require fundamental changes to the way the security controls are currently enforced. The following table summarizes the key security architecture considerations and requirements related to the integration with national system. The full list of security controls identified for the SIENA front end should be considered also for this system to system interface.

Control Category	Current situation	Considerations for the system to system interface
Authentication	Authentication controls are enforced by the SIENA front end. Password based authentication is used. A Central authentication LDAP based store is implemented for external users. User based authentication to the front end is performed.	User based authentication should be taken into account by national system. Only entity level authentication will be allowed (ie authentication of the entity initiating a service request). All service invocation must be authenticated. An new authentication solution must be developed
Access Control	Fine-grained access controls are implemented by the SIENA front-end. Access control is enforced based on the various user attributes including (OE, OSE and role).	The service interface should enforced access control decisions. Details access control rules should be defined for the new service interface. Service invocation only allowed for own OE or OSE.
Input and output validation	Input and out validation controls enforced through front end and backend	Input validation controls to be considered for the new service interface

Logging and Error Handling	All activities from the front end are logged using a dedicated audit system.	User based action logging should be implemented by the national system. the new service interface should include logging and error handling logic inline with the current implementation in the front end. All actions through this service interface should be logged through the audit system
Infrastructure controls	Web based access to SIENA application through the Reverse proxy placed in the Partner Access Zone	Service interface should be accessible via the reverse proxy. Infrastructure configuration (NATing, firewall rules, reverse proxy configuration) required to facilitate this. Bilateral agreements should be updated.