



Project co-funded by the  
CIVIL JUSTICE PROGRAMME  
Of the EUROPEAN UNION

# iSupport

cross-border recovery  
of maintenance obligations  
*pour le recouvrement transfrontière  
des obligations alimentaires*

## iSupport Privacy Impact and Security Assessment

<b>Project Name:</b>	iSupport		
<b>Date:</b>	2 November 2016	<b>Release:</b>	1.0
<b>Authors:</b>	Marie Vautravers		
<b>Owner:</b>	Philippe Lortie		
<b>Document Name:</b>	iSupport User Manual		

### Revision History

Revision Date	Version	Author	Reviewed by	Remarks
2 November 2016	0.2	Marie Vautravers	OCSE	Additional questions to Me-CODEX
5 May 2017	0.3	Jean-Marc Pellet		Clarifications received from Hiba Salma Additions related to GDPR

---

## iSupport

cross-border recovery of maintenance obligations  
*pour le recouvrement transfrontière des obligations alimentaires*

## Contents

Introduction.....	4
1 Scope .....	6
2 Need for a PIA.....	6
3 Risk analysis – methodology.....	7
4 Information flows .....	9
4.1 iSupport servers .....	9
4.2 Data sharing .....	9
5 Privacy and related risks and solutions .....	11
5.1 Risks to individuals .....	11
5.1.1 Proper and timely information of data subject.....	11
5.1.2 Risk in relation to the accuracy of data .....	13
5.1.3 Risk in relation to the retention of data .....	13
5.2 Applicable law .....	15
5.3 Appropriate security measures.....	17
5.4 Transferring personal data to non EEA countries .....	18
5.5 Associate organization risk - Contractual arrangements .....	19
5.5.1 Data controller and data processor.....	19
5.5.2 Contractual provisions relating to data protection between the data controller(s) and the data processor(s).....	19
6 iSupport security assessment.....	21

## Annexes

- Annex 1 Security and Data protection Scan
- Annex 2 Physical and logical data model
- Annex 3 RLSA Screen Design Specification Document
- Annex 4 NREF ScreeDesign Specification Document
- Annex 5 CCRT Design Specification Document
- Annex 6 System Certification Documentation Security and Privacy
- Annex 7 iSupport Questions PPT Presentation

## List of figures

Figure 1 iSupport architecture .....	10
Figure 2 iSupport simplified data flow outline .....	10
Figure 3 iSupport Screenshot. Notification of the defendant .....	20
Figure 4 SSL Certificates .....	22

## List of tables

**No table of figures entries found.**

DRAFT

## Introduction

The Hague Conference on Private International Law launched the iSupport project in September 2014, granted by the European Commission and supplementary funded by nine States and three organisations. The project aimed at developing an IT case management system to facilitate cross-border maintenance recovery. It has been developed for the process of applications and requests by Central Authorities designated under the 2007 Hague Child Support Convention and the 2009 EU Maintenance Regulation.

Led by the First Secretary of the Permanent Bureau of the Hague Conference responsible of the 2007 Hague Child Support Convention, and supported by an Advisory Board of experts as well as five Working Groups, the iSupport team has carried out an analysis of Central Authority needs under the two instruments and the delineation of a comprehensive legal and technical framework to develop, test and maintain iSupport early 2015.

It is expected that the progressive implementation of iSupport will be a significant milestone in implementing the 2007 Hague Child Support Convention and the 2009 EU Maintenance Regulation – and, indeed, more generally in improving the well-being of children around the world.

iSupport project documentation, including reports of the iSupport Advisory Board and Working Group meetings, is available on the [‘iSupport section’](#) of the Hague Conference website. For more information, e-mail [iSupport@hcch.nl](mailto:iSupport@hcch.nl).

**The Permanent Bureau has developed the iSupport software using a “privacy by design” approach which** promotes privacy and data protection compliance from the start. These issues are often bolted on as an after-thought or ignored altogether. Although this approach is not a requirement of the 1995 EU Directive, it will help participating States comply with their obligations under their local legislation. It also anticipates on the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as GDPR - General Data Protection Regulation). The Regulation also states that this privacy by design must be implemented *“taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing”*.

The GDPR will apply from 25 May 2018.

The HCCH has made his best efforts to ensure that privacy and data protection was a key consideration in the early stages of any project (Data protection working group), and then throughout its lifecycle.

Prior to the start of the project, both the 2009 Regulation and the 2007 Convention have established a strong legal and practical framework in relation to data protection. The 2007 Convention provides a greater protection in the event of domestic violence issues. Specific

## iSupport

cross-border recovery of maintenance obligations  
*pour le recouvrement transfrontière des obligations alimentaires*

provisions on the collection of personal data, the conditions of use and the duration of retention are set out in Article 61 and 62 of the 2009 Regulation. More generally, data shared between Central Authorities were strictly defined by the mandatory and recommended forms adopted under both instruments.

**To avoid any misunderstanding, it must be reminded that data processing and data control will be the sole responsibility of the States/authorities/bodies that implement the system, under their national applicable law and for EU States the EU data protection legislation.**

DRAFT

## 1 Scope

iSupport may only be used for specific purposes in relation with maintenance recovery applications made under the 2007 Hague Child Support Convention and the EU 2009 Maintenance Regulation, as well as other international agreements (such as the NY 1956 Convention) or bilateral agreements.

### **2007 Convention** - Article 2 Scope:

- to maintenance obligations arising from a parent-child relationship towards a person under the age of 21 years,
- to recognition and enforcement or enforcement of a decision for spousal support when the application is made with a claim within the scope of the previous paragraph.
- The EU, Albania and Norway have extended the scope of the Convention to spousal support.

### **2009 EU Regulation** Article 1 Scope of application:

- to maintenance obligations arising from a family relationship, parentage, marriage or affinity.

**Other instruments:** see each instrument specific scope.

**No binding instruments:** States agreeing to process between themselves child / spousal support applications on the basis of reciprocity (outside a Convention or bilateral agreement) will sign an agreement or proceed to an exchange of letters. It is recommended this agreement or letters include a specific scope and all data protection requirements.

## 2 Need for a Privacy impact assessment

iSupport involves the collection of information about individuals. Those individuals are the persons involved in a maintenance recovery case: persons for whom maintenance is sought (children or spouse), representatives of the persons for whom maintenance is sought, debtor. Other information related to the assets and financial status of each party may also be collected (employers, individuals sharing assets with the debtor). This information is mandated by European and international law (content of the 2009 Regulation and 2007 Convention forms), which ensures the collection is necessary and proportionate.

Applicants are required to provide required information to complete the application forms. Defendant may also be compelled to provide information on their financial/marital/personal situation.

iSupport will greatly facilitate the recovery of maintenance and will have an important impact on individuals (mainly increase the welfare of families and children around the world). The aim of the document is to ensure that the privacy impact is strictly related to the public's need for better maintenance recovery.

The information collected and shared through iSupport does not contain prohibited data according to Art. 9 of the GDPR or Art. 6 of Convention 108<sup>1</sup>. However, iSupport contains data

---

<sup>1</sup> <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>

that is potentially of interest for ill-intentioned persons: addresses of former spouses, information on income and financial situation. The address information is specifically protected under the 2007 Convention (Art. 40) and the 2009 Regulation (Art. 57) and this mechanism has been implemented in iSupport: a box indicating “non-disclosure” can be ticked and the corresponding forms will be generated without disclosing the personal address of the party concerned.

The information collected either through the individual himself or through competent authorities may be shared with the State where the other party resides or where assets are located.

All participants to iSupport (Central Authority, Service Provider and HCCH coordinator) are jointly responsible for the security of the system and its activities, including if any functions are subcontracted.

The HCCH makes sure that iSupport complies with the standard software security requirements. It means that a risk analysis has been performed (please see below 3. Risk analysis), and relevant technical security measures have been implemented in the Software.

Central Authorities will be the data controller (please see 6.5.1) and therefore responsible for personal data security. Central Authorities will thus be responsible for implementing organisational security measures under their national law. Those security measures are identical to any security measures implemented for IT software used by the Central Authority. They will imply for instance keeping password and user ID in a safe place not for public view, and maintaining the iSupport user list in a timely and efficient manner.

The Service Provider will provide maintenance also in relation with security matters as directed by the HCCH, and will provide staff members with a restricted access to iSupport information only in accordance with the terms and conditions of the Maintenance Contract (See 6.5.2). Any production issues should be replicated in the test environment reducing the need for access to production data.

### 3 Risk analysis – methodology

Prior to the development of the system, the Permanent Bureau has set up a Data Protection Working Group in order to identify and address data protection and security issues such as access rights and user profiles, external access, logging of changes and views, database encryption, European Data Protection Regulation etc.

This Working Group was comprised of several data protection experts and has met twice by videoconference on 15 January and 12 February 2015. [Meeting reports](#) are available on the iSupport webpage.

All-important findings and recommendations of the Working Group have been incorporated as “Must Have” requirements into the Deliverables Documents aimed at potential tenderers that was released on 2 April 2015 under the call for tender.

---

## iSupport

According to the decision of the Data Protection Working group, a security and data protection working group met twice during the development of the system to undertake a security scan and ultimately draft this report (see Annex 1).

Further to the recommendation of the Data Protection Working Group, Data Protection experts have been consulted by the Council of Bars and Law societies of Europe (CCBE) who has produced a questionnaire on Data Protection listing all existing concerns and possible issues. This questionnaire and the answers provided by the Permanent Bureau have been reviewed by all stakeholders and are included in this report.

DRAFT



## 4 Information flows

### 4.1 iSupport servers

iSupport related servers are all located on the State local environment. Those servers will store all functional and technical data required to run the system.

Please see **Annex 2**: Physical and Logical Datamodel

### 4.2 Data sharing

Data transferred **from a country to another** will be of two different types:

- Data contained in the forms (most common cases). 2009 European Regulation forms as well as 2007 Convention mandatory and recommended forms have been agreed upon by Member States of the European Union and State parties to the Convention respectively. For other international or bilateral instruments, or even reciprocity based exchanges, neutral forms have been developed on the model of Convention forms. The use of neutral forms will guarantee that only data required for maintenance recovery is transferred. Data contained in the Forms is solely related to the purpose of maintenance recovery.
- Information exchanged via letters or emails (less frequent). This data cannot be subject to a specific control and are not stored per se in the system.

Data **provided by national competent authorities** to Central Authority is exchanged/processed by EU Central Authorities under articles 61 and 62 of the 2009 Regulation.

Domestic law will apply to internal data flows outside of the EU.

Within Central Authorities, staff members can be provided with different access rights depending on their role (manager, caseworker, accountant, registrar and any specific role created by a Central Authority). Those staff members will be granted with “view”, “update”, “add” and “delete” rights that will vary depending on the iSupport screens. iSupport RLSA screen allows the creation and modification of roles and access rights on an extremely flexible basis (see Annex 3 RLSA DSD).

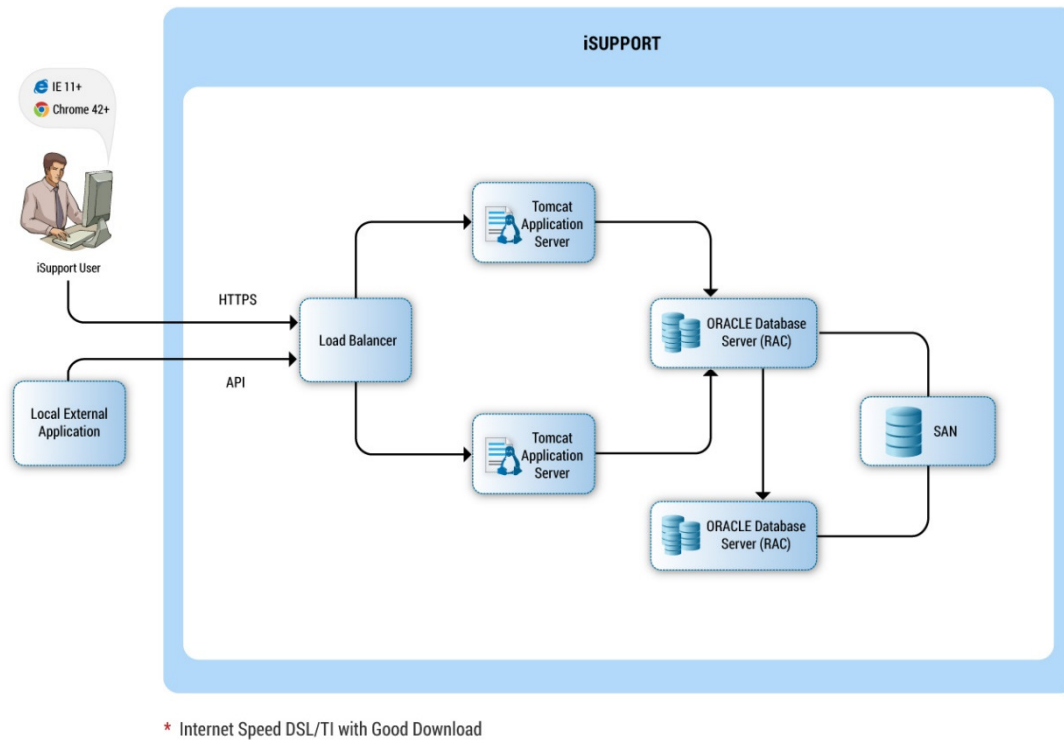


Figure 1 iSupport architecture

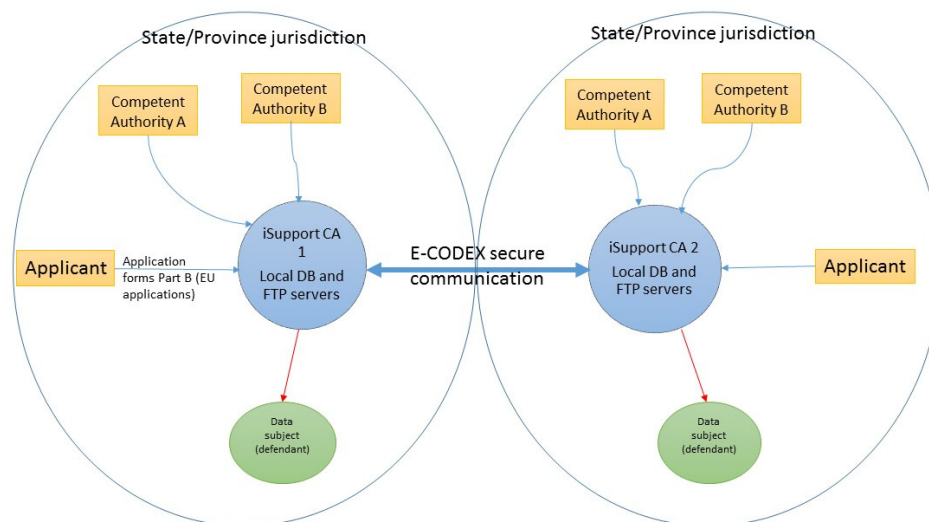


Figure 2 iSupport simplified data flow outline

## iSupport

cross-border recovery of maintenance obligations  
pour le recouvrement transfrontière des obligations alimentaires

## 5 Privacy and related risks and solutions

### 5.1 Risks to individuals

#### 5.1.1 Proper and timely information of data subject

- Will the data subject be informed that their personal data are being processed, for which purpose and how?

Each Central Authority will inform the data subject under the applicable data protection legislation. Different legal requirements may apply. As a minimum best practice, the Central authority should provide the data subject with the following information:

- The fact that their personal data may be processed in iSupport
- The identity and contact details of the controller (i.e. those of the Central Authority)
- The categories of recipients to whom the data may be disclosed (i.e. competent authorities in the requested and requesting States).
- The right to access their personal data and to have it corrected.

Templates letter to the applicant/defendant can be associated to one particular task in the activity list/edited to display specific appropriate notification. (See Annex 4 NREF Screen DSD)

The 2009 Regulation provides specific provisions with regard to the processing of the defendant's personal data.

*"Article 63 Notification of the data subject*

*1.Notification of the data subject of the communication of all or part of the information collected on him shall take place in accordance with the national law of the requested Member State.*

*2.Where there is a risk that it may prejudice the effective recovery of the maintenance claim, such notification may be deferred for a period which shall not exceed 90 days from the date on which the information was provided to the requested Central Authority."*

This maximum deadline of 90 days has been implemented in iSupport Regulation cases as a reminder to inform the data subject when information is provided by a competent authority.

- Will the data subject be informed of his / her right of access (recital 34 Regulation) and duly notified in conformity with Article 63 Regulation?

CF Answer to the question above. (It is for each CA to determine the content of the data subject notification)

- Will the data subject be informed about the people or organisations his / her data may be passed onto?

CF Answer to the question above.

- [Will the iSupport system enable authorities to comply with the non-disclosure and confidentiality requirements set out in Articles 39 and 40 of the Convention, and Article 61 Regulation?](#)

When the health, safety or liberty of a person is at risk, the case-worker ticks the non-disclosure box, and sensitive information will not be transmitted, in compliance with Articles 39 and 40 of the Convention and 57 of the 2009 Regulation. The generation of the adequate form is automatic when sending out the application.

A “Non-disclosure” notice is displayed in the case summary ribbon, as well as in the case management screen and in the debtor and creditor demo screens.

Pursuant to Article 61(2) of the 2009 Regulation, caseworkers will have the ability to only disclose the information which is adequate, relevant and not excessive. Mandatory EU forms have been designed for this purpose.

Next releases might provide further guidance in that respect.

- [Do I need the prior consent of data subject before processing their information?](#)

Personal data are processed in iSupport on the basis of specific provisions of the 2009 Regulation and 2007 Convention, therefore it's not necessary to ask for the data subject's consent in order to justify the processing. This is in line with the article 7 of the data protection Directive 95/46/EC (exception for “*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed*”) and Article 16 GDPR.

Moreover in Regulation cases, the applicant's personal data is only contained in Part B which is filled by the applicant.

As for Convention cases, Article 12 (2) provides that the Central Authority transmits the application “*on behalf and with the consent of the applicant*”. In that view, recommended forms include a tick box indicating that “*This application is forwarded by the Central Authority on behalf of and with the consent of the applicant*”.

- [If the data collection includes sensitive data, will explicit consent to process such data be required from the data subject?](#)

“Sensitive data” needs to be further defined. The GDPR prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. According to this definition, applications made under the Convention and / or the Regulation do not include sensitive data.

iSupport does not contain fields related to such data.

Specific provisions have been set out for family violence cases (please see above).

- [Will it be made clear to the data subject what the data will be used for?](#)

Applicants are aware of the purpose of their own application, and the range of possible use of the data is extremely restricted.

---

## iSupport

cross-border recovery of maintenance obligations  
*pour le recouvrement transfrontière des obligations alimentaires*

More generally, States and Central authorities are responsible for the actual notification of the data subject, which will be documented by the attestations found in the forms transmitted.

- Will any "non-obvious uses" of the data be made clear to the data subject i.e., things that the data subject cannot realise iSupport will do from a general description of the processing?

Applications are exclusively made for maintenance recovery purposes. iSupport processes are extremely straightforward and clear. In that respect, there are no "non-obvious use" of data. Data will only be sent out to other Central Authorities.

States will be responsible for ensuring that this data is not used for any other purpose unless the data subject is informed and can give his prior consent.

**2009 EU Regulation, Article 62:** *Any authority or court to which information has been transmitted pursuant to Article 61 may use this only to facilitate the recovery of maintenance claims.*

Templates of letters sent to competent authorities and courts can make reference to Article 61 2), 3) and 4).

**2007 Convention, Article 38:** *Personal data gathered or transmitted under the Convention shall be used only for the purposes for which they were gathered or transmitted.*

#### 5.1.2 Risk in relation to the accuracy of data

- What steps will be taken to ensure the accuracy of the data?

Change Logs will be kept in the system, which will ensure data integrity. All actor information can be updated in the dedicated screens (demographics and addresses).

- Is there a system of rolling reviews of data to keep the data up to date?

Periodical review of cases will be the responsibility of States. An automatic reminder for caseworker to review the case has been implemented in iSupport after six months of inactivity in a case. This time period can be modified.

#### 5.1.3 Risk in relation to the retention of data

- Is the data being kept for no longer than is necessary to comply with relevant laws and regulations that define minimum periods of retention?

As already stated, iSupport prompts caseworkers to review periodically cases that are no longer active (by default every six months). Cases can be closed (in that case they are no longer editable) or archived (in that case, data is removed from iSupport to a separate database: only basic information will be kept such as the iSupport and internal number, the debtor and persons for whom maintenance is sought full name and date of birth). Data management,

---

## iSupport

cross-border recovery of maintenance obligations  
*pour le recouvrement transfrontière des obligations alimentaires*

including case review, closure and archiving procedure will depend on domestic legal requirements.

- [Can it be confirmed that data is not being kept on a "just in case" basis?](#)

On the condition that relevant processes have been implemented in iSupport, and that periodical reviews are performed, cases should be archived on time.

DRAFT

## 5.2 Applicable law

- [How will the solution be "future proofed" to ensure compliance with the General Data Protection Regulation?](#)

The iSupport solution complies with the 2009 Regulation data protection requirements and more generally with the data protection EU Directive 95/46/EC.

EU Regulation 2016/679 will apply from 25 May 2018. It promotes a risk-based approach, with security measures in proportion to those risks. Most of its innovations centre on commercial activities, therefore outside of iSupport's scope. Consent of the data subject is not necessary as "*processing is necessary for compliance with a legal obligation to which the controller is subject*" and "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*".

iSupport does not handle any prohibited data according to Art. 9.

Art.13 lists the information that should be provided where personal data are collected from the data subject (addition from the Directive in italics):

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- The contact details of the data protection officer, where applicable;
- The purposes of the processing for which the personal data are intended as well as the *legal basis* for the processing;
- The recipients or categories of recipients of the personal data, if any;
- Where applicable, the fact that the controller *intends to transfer personal data to a third country or international organisation* and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
- *The period for which the personal data will be stored*, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from the controller access to and rectification or *erasure of personal data or restriction of processing concerning the data subject*;
- The right to lodge a complaint with a supervisory authority.

Slightly more information must be provided where personal data have not been obtained from the data subject, as listed in Art. 14 (this was already present in the Directive): the categories of data concerned; from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

Right of access can be obtained at reasonable intervals and free of charge. It should also be noted that the controller should implement reasonable measures to verify the identity of a data subject who requests access.

Rectification can be obtained from the controller without undue delay.

The right of erasure and to be forgotten shall be granted without undue delay when the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; when the data subject withdraws consent and there is no other legal ground for the processing of the data; when the data have to be erased for compliance with a legal obligation to which the controller is subject.

The right of erasure is balanced with the right of freedom of expression and information and the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

---

## iSupport



There is also a right to restriction of processing where the accuracy of the data is contested by the data subject; where the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.

Provisions on the transfer of data to third countries and international organisations are also very much in the continuity of the Directive. The basis for the transfer can either be an adequacy decision of the European Commission or a legally binding and enforceable instrument between public authorities or bodies.

- Under which national law(s) will data be stored?

Each iSupport instance database is located in the State that will be responsible for ensuring compliance with the applicable domestic law.

- Which jurisdiction's data protection law(s) will apply and will the solution be compliant with each of these laws?

**Data management within Central Authorities as well as data import from other national competent authorities** are the responsibility of the State, in compliance with its national law and jurisdiction rules.

2007 Convention, Article 39 Confidentiality: *"Any authority processing information shall ensure its confidentiality in accordance with the law of its State".*

2009 EU Regulation, Article 62.4: *"Any authority processing information communicated to it pursuant to Article 61 shall ensure the confidentiality of such information, in accordance with its national law."*

In that respect, iSupport is extremely flexible and allows any adjustment locally required. For instance, iSupport does not allow the permanent deletion of data except for archiving purpose and therefore ensures appropriate access right of the data subject to his personal data.

In addition, as already indicated access rights and archiving procedure and deadlines (See Annex 5 CCRT DSD "Modify mode" "case tab" p. 42) are customizable depending on each State domestic data protection rules.

**Cross-border data flows** will mainly occur through Regulation and Convention forms. States that implement and use iSupport have agreed to the administrative cooperation and the transfer of data for the purpose of maintenance recovery.



### 5.3 Appropriate security measures

- Is the level of security adopted appropriate to the risks represented by the processing and the nature of the data to be protected?

It is to each Central Authority to implement measures to guard against theft, malicious damage or corruption (including computer viruses), unlawful access, accidental disclosure, loss and destruction. Particular consideration should be given to the security of sensitive data.

As regards security technical requirements, please see the System Security Documentation provided by Protech (Annex 6).

- What security accreditations (for example, ISO 27001/2) does the service provider hold?

The service provider responsible for the maintenance of the system (Protech) is a CMMI Level 3 organization, which is a certification from Carnegie Mellon University.

## 5.4 Transferring personal data to non EEA countries

Where applicable, will the consent of the data subject be obtained to transfer personal data to countries outside the EEA which are not designated as "adequate" by the European Commission?

(please see 5.2 Applicable law).

The derogation set out in Article 46(1)a of the GDPR applies. No adequacy decision is required as long as the data transfer is legally required on important public interest grounds and for the establishment, exercise of legal claims. Applications made and sent through iSupport under a binding international legal instrument fall under that category.

## 5.5 Associate organization risk - Contractual arrangements

### 5.5.1 Data controller and data processor

The Central Authority using iSupport will be the Data processor.

The Data controller is the natural or legal person, public authority, agency or any other body appointed in each State using iSupport. The identity of the controller cannot be predicted and will depend on each State's policy.

The identification of the data controller and possibly data processor may be included in the agreement signed by States implementing iSupport after the Pilot phase.

As long as Central Authorities do not subcontract the processing of personal data, Data processor and Data controller will be the same. If they subcontract the provision of Servers and other IT services for the purpose of iSupport implementation, this will be their responsibility to sign a contract with the contractor and identify his data protection duties.

### 5.5.2 Contractual provisions relating to data protection between the data controller(s) and the data processor(s)

The Service provider might have access to personal data and specific contractual provisions that have been set out in that respect. In the iSupport Maintenance Contract:

#### **Article 32. Processing of personal data**

84. *Where the Contract requires the processing of Personal Data by the Contractor, the Contractor may act only under the explicit direction of the Contracting Authority, in particular with regard to the purposes of the processing, the categories of data which may be processed, the recipients of the data and the means by which the data subject may exercise his rights.*

85. *The Contractor shall grant its Personnel access to the data to the extent necessary for the performance, management and monitoring of the contract.*

86. *The Contractor undertakes to adopt all technical and organisational security measures that are necessary to protect all Personal Data that are under its direct or indirect control during the course of this Contract and the Contractor agrees and warrants that it will:*

- a) Ensure the compliance of the Software with the European Legislation on protection of Personal Data and any relevant domestic legislation for any State in which it is providing services or where the Solution is being developed or tested;*
- b) Ensure all of its personnel are properly screened and adequately trained concerning the legislative and contractual requirements concerning the protection of personal data required by this Contract;*
- c) Take all required precautions to prevent any unauthorised person from gaining access to any computer systems that is processing personal data;*
- d) Ensure that authorised users of the Solution during the development and deployment of the Solution can access only the personal data to which their access rights refer;*
- e) Develop the Solution strictly in compliance with the Deliverables Document requirements concerning personal data; and*

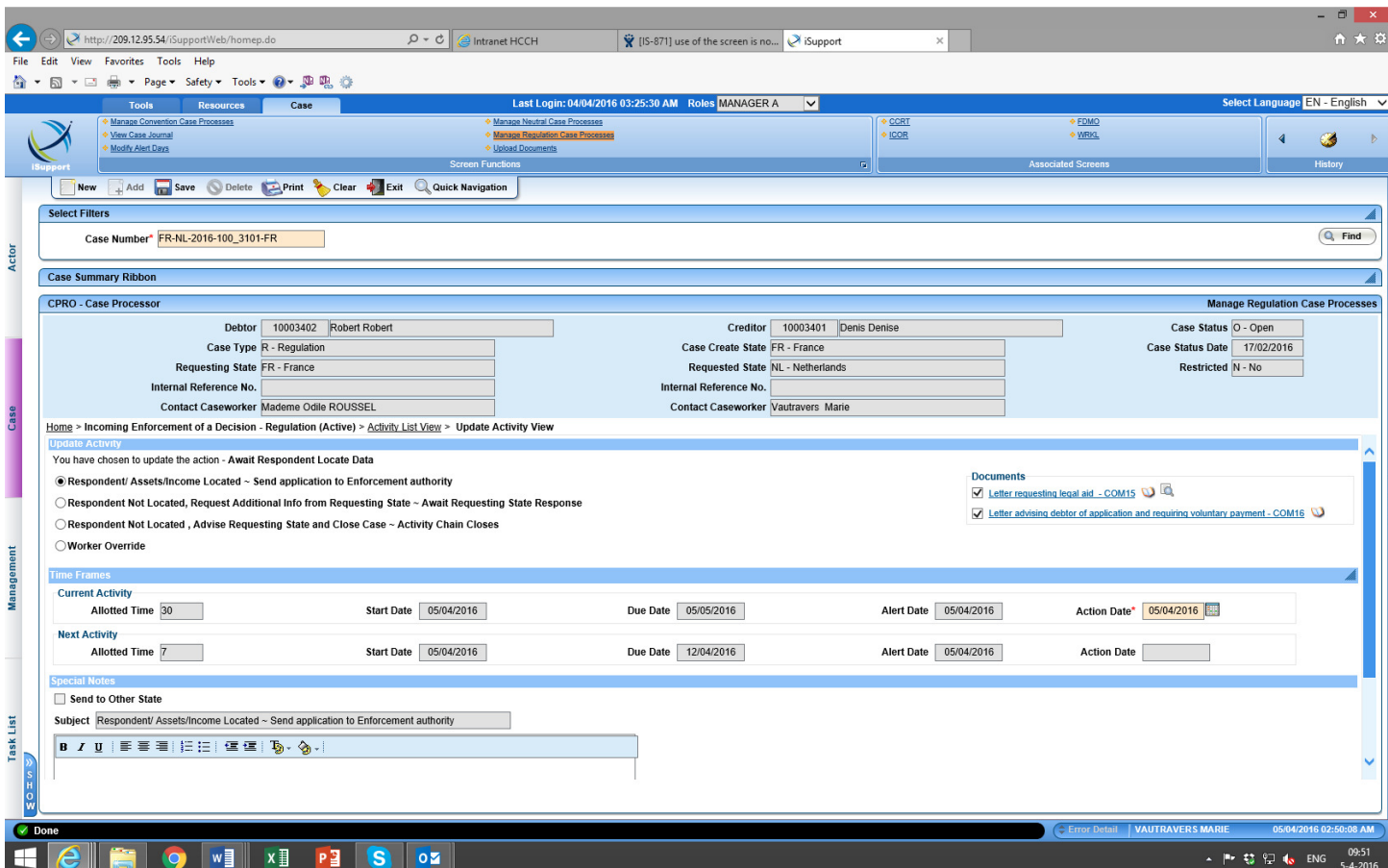
---

## iSupport

f) *Ensure that the Solution provides that any personal data being processed on behalf of third parties can be processed only in the manner prescribed by the Contracting Authority.*

Notification of the data subject automatic when data is communicated.

In future versions, automatic notification of data subject in his own language will be implemented. Currently, the word document has to be manually edited, or another existing local letter has to be sent.



The screenshot displays the iSupport web application interface. The top navigation bar includes 'Tools', 'Resources', and 'Case' tabs. The 'Case' tab is active, showing a 'Case Summary Ribbon'. The case details are as follows:

Debtor		Creditor		Case Status	
10003402	Robert Robert	10003401	Denis Denise	O - Open	
Case Type: R - Regulation		Case Create State: FR - France		Case Status Date: 17/02/2016	
Requesting State: FR - France		Requested State: NL - Netherlands		Restricted: N - No	
Internal Reference No.:		Internal Reference No.:			
Contact Caseworker: Madame Odile ROUSSEL		Contact Caseworker: Vautravers Marie			

Below the case details, there is a section for 'Update Activity' with the following options:

- ☒ Respondent/ Assets/Income Located - Send application to Enforcement authority
- ☐ Respondent Not Located, Request Additional Info from Requesting State - Await Requesting State Response
- ☐ Respondent Not Located, Advise Requesting State and Close Case - Activity Chain Closes
- ☐ Worker Override

The 'Time Frames' section shows the following dates:

Activity	Allotted Time	Start Date	Due Date	Alert Date	Action Date
Current Activity	30	05/04/2016	05/05/2016	05/04/2016	05/04/2016
Next Activity	7	05/04/2016	12/04/2016	05/04/2016	

The 'Special Notes' section includes a checkbox for 'Send to Other State' and a text area for 'Subject: Respondent/ Assets/Income Located - Send application to Enforcement authority'.

Figure iSupport Screenshot. Notification of the defendant

## 6 iSupport security assessment (Questions and answers)

**Please refer to the relevant slides of Annex 7.**

1. **Architecture of the e-CODEX Gateway (slide 3)** – Who will configure the eCODEX Backend Integration module?

This is part of the Gateway installation package.

2. **Preparation for going live (slide 7)** - How will the eCODEX endpoint IP addresses be exchanged?

The IP addresses will be exchanged via email.

3. How will the ebMS Gateway certificates be obtained?

The GW stores the certificates for the partner GW in a separate truststore. This truststore will be created together with the p-mode files

4. How will the ebMS Gateway certificates be exchanged?

The public certificates will be sent, together with the other configuration parameters, to the iSupport CfC.

The CfC creates the config files (p-modes, truststore) and provides them to all iSupport GW hosting authorities. Updated config files will be made available on the iSupport Platform and an alert will be sent to all iSupport users (a dedicated email address list must be provided by users).

5. Do these certificates expire?

Yes. The GW hosting authority is responsible for monitoring the certificate lifetime and timely inform the iSupport CfC.

6. How will the SSL certificates be obtained?

This issue of the SSL certificates is not specific for e-CODEX, and will be similar to the issue of certificates for other infrastructures.

7. How will the SSL certificates be exchanged? Where are external SSL connections terminating? On the proxy server or the application server? How are the SSL certificates going to be exchanged with other states?

They are exchanged through p modes. (see Answer 4). SSL certificates are usually loaded onto the proxy server, not the application server. The proxy or the webserver in front of the Domibus application server handles the SSL verification on the server side (receiving side). On the client side (sending side) the Domibus GW establish the SSL connection and verifies the authenticity of the received server certificate.

For this purpose the trust store containing all server certificates for verification must be configured in the GW property `domibus.ssl.truststore.path` in the file `DOMIBUS-HOME/conf/Catalina/localhost/Domibus.xml`.

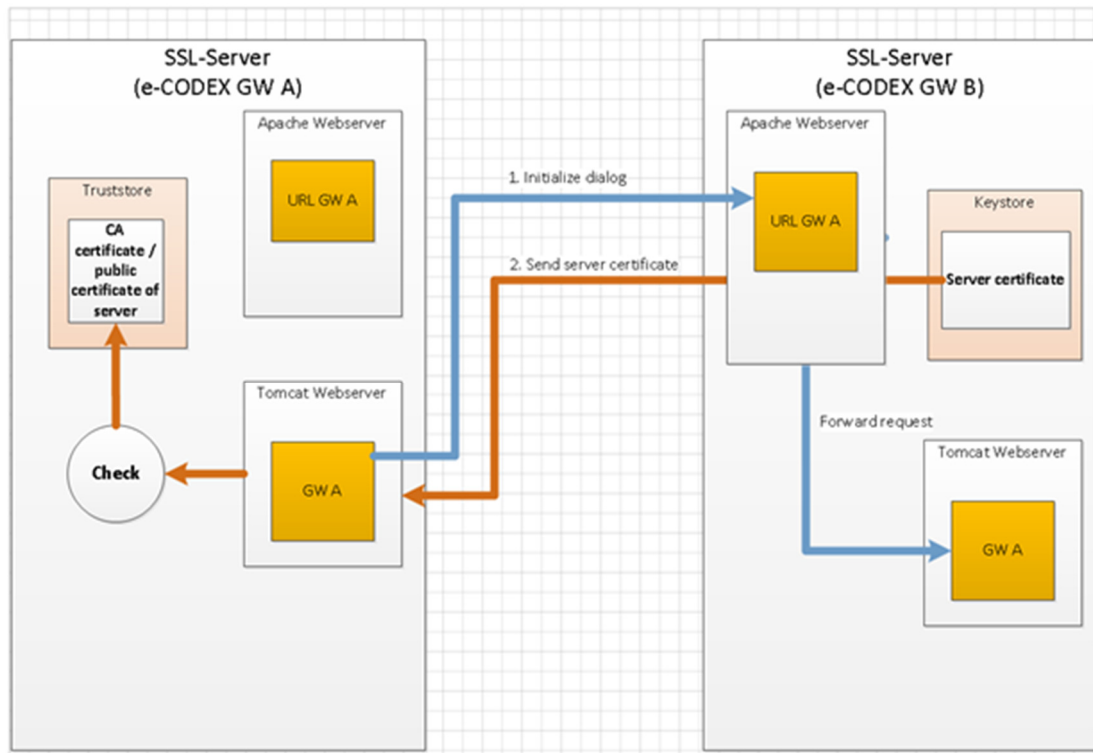


Figure 3 SSL Certificates

8. Do these certificates expire? Once the SSL certificates expires, are we getting new certificates to be loaded on our proxy server?

SSL certificates can expire indeed. (see Answer 5). A new release of configuration files for the iSupport States will be created, containing a trust store file for the server verification, if a SSL certificate of a State expires.

9. Will all SSL communications use TCP port 443?

No, it can be another one as well

10. **Digital signature (slide 8)** - What digital signature algorithms will be used for eCODEX?

The Domibus GW expects the algorithm <http://www.w3.org/2001/10/xml-exc-c14n#> Domibus 3 and later use SHA256.

11. Will eCODEX use Certificate Revocation Lists (CRL)?

No

12. Will eCODEX use Online Certificate Status Protocol (OCSP)?

No

## iSupport

cross-border recovery of maintenance obligations  
pour le recouvrement transfrontière des obligations alimentaires

13. Where will eCODEX store the SSH key for SFTP?

No, SFTP is not a specific feature for the Domibus GW.

14. How will the SSH key be stored in eCODEX?

The file system location can be configured within the Domibus installation. Config file: [DOMIBUS\_ROOT]/ domibus/conf/Catalina/localhost/Domibus.xml

15. Ref slide 3 – Will eCODEX only interface with the SFTP server for the National Subsystem?

There is no SFTP interface for Domibus.

16. Does eCODEX use DNS?

Domibus supports URL as endpoint address, the version 3.1 of Domibus also supports dynamic discovery. URLs and IP addresses can be used and DNS is fully supported.

17. Does eCODEX send emails?

No

18. Does eCODEX have administration modules via web pages?

No users, only certified organisations but in the case of iSupport this is always iSupport.

19. Should eCODEX be deployed separately from iSupport as shown in diagram in page 2?

They *can* be installed in two different environments, but it is not mandatory to use a firewall between the iSupport and the e-CODEX environment. Each has its own installation procedure.

20. Is data encrypted in iSupport/e-CODEX?

Data is all encrypted in transit.

iSupport uses RSA algorithm with key size of 1024. iSupport: Encryption takes place within iSupport's application layer. Public and private keys (the public keys of course needs to be shared with the other iSupport States). By default e-CODEX only uses normal Server authentication (1-way-SSL)

In transit (e-CODEX): 2-way-SSL for the communication between Gateways if the other iSupport State also uses 2-way-SSL. 2-Way SSL is optional but can be configured. Otherwise Domibus is using 1 way SSL. This is just the encryption on the transport layer, on the application layer, the message is being encrypted by e-codex as well (to be implemented at the time of writing).