Projet cofinancé par le
PROGRAMME DE JUSTICE CIVILE
De l'UNION EUROPEENNE

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

Groupe de travail iSupport sur les communications sécurisées (e-CODEX) (3) et sur les exigences techniques (2)
Jeudi 12 Mars 2015, 15h00 UTC (16h00 ECT)

Liste des participants (et heure locale de la vidéoconférence)

Experts

Robert BLUKIS (Lettonie - 17h00)
Mary BUTLER (Etats Unis d'Amérique – 07h00)
Natasha BUTLER (France – 16h00)
Enrico FRANCESCONI (ITTIG – 16h00)
Lesli HOMMIK (Estonie – 17h00)
Sven JENSEN (Estonie – 17h00)
Torsten KIRSCHNER (Norvège – 16.00)
Hannah ROOTS (NCSEA – 8h00)
Casten SCHMIDT (e-CODEX – 16.00)
Eduardo SPANO JUNQUEIRA DE PAIVA (Brésil – 13h00)
Thomas STEIMER (Suisse – 16h00)

Equipe iSupport

Philippe LORTIE
Brigitte VOERMAN
Juliane HIRSCH
Marie VAUTRAVERS
Patrick GINGRAS

Objectifs du groupe de travail sur les communications sécurisées (e-CODEX) (3) :

En reprenant les avis fournis par le Comité consultatif, analyser et prendre des décisions au sujet de la mise en œuvre d'e-CODEX comme un moyen de communication sécurisé pour le système de gestion des dossiers et de communications sécurisées iSupport.

Objectifs du groupe de travail sur les exigences techniques (2) :

En reprenant les avis fournis par le Comité consultatif, analyser et prendre des décisions au sujet des questions techniques du système de gestion des dossiers et de communications sécurisées iSupport.

Ordre du jour

1. **Appel nominal et remarques introductives**

2. **e-CODEX – Questions en suspens – Accord sur l'utilisation d'e-CODEX**

3. **Suivi de la dernière réunion du groupe de travail sur les exigences techniques**

   - Types de documents utilisés par les Autorités centrales, par exemple PDF, Word ou ODT (LibreOffice, OpenOffice)
   - Liste des applications (Java, etc.) utilisées par les Autorités centrales
   - Open Web Application Security Project (OWASP - https://www.owasp.org/index.php/Cheat_Sheets), en particulier SQL Injection Prevention ou Cross Site Scripting Prevention

4. **Autres sujets de discussion**