Study on Online Collection Systems and technical specifications pursuant to Regulation 211/2011 and Implementing Regulation 1179/2011

DIGIT B.2

2 June 2017
ECI Technical Specifications

Agenda

- Context and objectives
- Presentation of the technical scenarios under assessment
  1. Stand-alone OCS under the responsibility of the organisers
  2. OCS software and hosting only provided by the Commission
  3. OCS as a single central online platform
- Methodology
- Assessment
ECI Technical Specifications

Context and objectives

Context

(i) Revision of the ECI Regulation

(ii) In particular, scenario 3 of this study (i.e. single central online platform managed by the Commission) could lead to additional benefits in the light of the study on the use of electronic identification.

Objectives

(i) Assess the 3 scenarios from legal, business, technical and security perspectives

a. Under scenario 3, investigate the possible integration with the Commission ECI Register and the impact of additional features (i.e. use of e-TrustEx), and provide high-level IT architecture

(ii) Propose recommended changes to Regulation 211/2011 and Implementing Regulation 1179/2011 in order to make the functioning of the online collection simpler, more efficient and fit for purpose
ECI Technical Specifications

Scenario 1 – Standalone OCS under the responsibility of the organisers

This scenario consists in the update of the current technical specifications to cater for evolution and new threats in security as well as in application architecture. **Standalone instances of OCS software and infrastructure** can be provided either by the Commission or by third party hosting organisation.
ECI Technical Specifications
Scenario 2 – OCS software and hosting only provided by the Commission

This scenarios evaluates the feasibility and impact of allowing only the current Commission OCS software and infrastructure for collecting statements of support, from a legal, business, technical, and security perspective. Each OCS is provided as a standalone instance.
This scenario evaluates the feasibility and impact of providing the **OCS** as a single central online platform managed by the **Commission** in a **cloud-based centralised environment**, from a legal, business, technical, and security perspective.
Phase 1: Description

Scenario 1
Scenario 2
Scenario 3

Phase 2: Analysis

Legal Business Technical Security Evaluation criteria

Phase 3: Assessment

Evaluation Matrix SWOT Analysis Comparison Conclusions and recommendations
The 3 scenarios will be assessed according to 4 dimensions and a total of 12 criteria:

- Legal
- Business
- Technical
- Security

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Legal Analysis</th>
<th>Business Analysis</th>
<th>Technical Analysis</th>
<th>Security Analysis</th>
<th>Score</th>
</tr>
</thead>
</table>
| Scenario 1  
Stand-alone OCS under the responsibility of the organisers | ECI Regulation | GDPR Regulation | Convenience | Certification | Verification | Implementation | Operations | Costs | Security Architecture | Software Development | Development Security | Data Security & Integrity | Identity & Access Management | TOTAL SCORE |
| Scenario 2  
OCS software and hosting only provided by the Commission | ECI Regulation | GDPR Regulation | Convenience | Certification | Verification | Implementation | Operations | Costs | Security Architecture | Software Development | Development Security | Data Security & Integrity | Identity & Access Management | TOTAL SCORE |
| Scenario 3  
For each dimension, the impact on every stakeholder is assessed in order to obtain a score for each scenario.

In addition, a SWOT analysis will be performed to highlight the pros and cons of each scenario.
## ECI Technical Specifications
### Assessment of the Solutions

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Scenario 1</th>
<th>Scenario 2</th>
<th>Scenario 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal analysis</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECI Regulation</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td>GDPR Regulation</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td><strong>Business analysis</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Convenience</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td>Certification</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td>Verification</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td><strong>Technical analysis</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td>Operations</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td>Costs / efforts</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td><strong>Security analysis</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Architecture</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td>Software development</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td>Data Security &amp; Integrity</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
<tr>
<td>Identity &amp; Access Mgmt</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
</tr>
</tbody>
</table>
Any questions or comments, please contact the everis team:

Monika Kokstaite monika.kokstaite@everis.com

Cédric Genin cedric.genin@everis.com

+32 2 788 52 52