cessda saw

Research and Innovation Action

CESSDA Strengthening and Widening

Project Number: 674939 Start Date of Project: 01/08/2015 Duration: 24 months

# Deliverable 4.4 - Report on DSA Certification for CESSDA

| | |
|---|---|
| Dissemination Level | PU |
| Due Date of Deliverable | 01/09/2017 |
| Actual Submission Date | 27/10/2017 |
| Work Package | WP4 |
| Task | T4.3 |
| Type | Report |
| EC Approval Status | 16 November 2017 |
| Version | V1.0 |
| Number of Pages | p.1 – p.39 (+ Appendix) |

**Abstract:** In this final report, the two key issues covered by task 4.3 of the SaW project are addressed and evaluated:

- Provide support, assistance and monitoring of progress by all CESSDA Service Providers (SPs) towards compliance with Trustworthy Digital Repository (TDR) requirements
- Map the CESSDA Annex II obligations



Project funded by the EU Horizon 2020 Research and Innovation Programme under the agreement No.674939

# History

| Version | Date | Reason | Revised by |
|---|---|---|---|
| V0.1 | 18/08/2017 | First draft | Heiko Tjalsma (DANS) |
| V0.2 | 24/08/2017 | Second draft with contributions by Mari Kleemola (FSD), Natascha Schumann (GESIS) and Janez Štebe (ADP | Heiko Tjalsma (DANS) |
| V0.3 | 29/08/2017 | Third draft with contributions by Hervé l'Hours (UKDA) | Hervé l'Hours (UKDA) |
| V0.4 | 20/09/2017 | Fourth draft with contributions by Hervé l'Hours (UKDA) | Hervé l'Hours (UKDA) and Heiko Tjalsma (DANS) |
| V1.0 | 24/10/2017 | Final draft | Heiko Tjalsma (DANS) |

# Author List

| Organisation | Name | Contact Information |
|---|---|---|
| DANS | Heiko Tjalsma | Heiko.tjalsma@dans.knaw.nl |
| UKDA | Hervé l'Hours | herve@essex.ac.uk |
| FSD | Mari Kleemola | Mari.Kleemola@staff.uta.fi |
| GESIS | Natascha Schumann | Natascha.Schumann@gesis.org |
| ADP | Janez Štebe | Janez.Stebe@fdv.uni-lj.si |

# Time Schedule before Delivery

| Next Action | Deadline | Care of |
|---|---|---|
| Review by the task partners | 25/10/2017 | DANS |
| Review by the WP leader | 26/10/2017 | DANS |
| Review by the Chair of the Delivery Committee | 26/10/2017 | CSDA |
| Review by the Project Coordinator | 27/10/2017 | CESSDA |
| Approval and Submission by the Project Coordinator to the European Commission | 27/10/2017 | CESSDA |

# Executive Summary

The two key issues covered by task 4.3 of the SaW project were:

1. Provide support, assistance and monitoring of progress by all CESSDA Service Providers (SPs) towards compliance with Trustworthy Digital Repository (TDR) requirements, by undertaking CESSDA-internal peer-review of self-assessments against the CoreTrustSeal (formerly Data Seal of Approval-DSA)
2. Map related concepts between the CESSDA Annex II obligations and the TDR requirements

The work on these two issues, carried out during the SaW project, is addressed in this report. Task 4.3 was carried out by the existing Trust Working Group of CESSDA (further: Trust Group) as the objectives of this task concurred with those of the Group. For the duration of the work the activities of the Trust Group were fully undertaken through the work package and task. The Group will continue these activities after the end of the project.

*The first task* was directed at the certification of all SP's as trustworthy digital repositories by complying with the CoreTrustSeal. CESSDA mandated compliance with the CoreTrustSeal (then DSA) in 2014. This SaW task broadly mirrored the approach taken within CESSDA to inform and support SPs on TDR issues in 2013: through cooperation within and between all SP's and in particular by creating, sharing and reviewing test self-assessments. This led to discussions on the TDR requirements, to the production and presentation of self-assessments by most SP's, evaluation through an anonymised gap analysis and an intense consultancy on a one-to-one basis. Cooperation between SP's was supported by the identification of a key TDR contact from each SP which worked with the T4.3 group.

The transition of the requirements from Data Seal of Approval (DSA) to CoreTrustSeal during the course of the SaW project presented some complications and delays even though the fundamental focus of the requirements remained the same. Nevertheless, in September 2017, more than half of the 24 involved CESSDA SP's have almost reached certification: ten have either acquired the seal or submitted their self-assessment and another five can reasonably be expected do so within one or two years (see the table in chapter 4 of this deliverable). Of the nine SP's who have not achieved this it can be said that most of them are SP's which are starting and, consequently, will not be able do that soon. In this report, it is analysed why complying with the CoreTrustSeal requirements is not a straightforward easy and, in particular, quick task

to perform and certainly not for SP starters. It also shows which requirements are easier to fulfil than others.

The conclusion here is that achieving the mandatory TDR Certification across all SP as envisaged by the Annex II obligations of the CESSDA Statutes will be an ongoing process for current and aspiring SPs. As well as providing ongoing guidance and consultancy through established SP contacts, as foreseen in the 2018 working plan for CESSDA, the Trust Group will also monitor changes to the TDR landscape including any changes to the CoreTrustSeal processes and requirements.

*The second task*, to map related concepts between the CESSDA Annex II obligations and the TDR requirements, proved to be quite complex. Many of the CESSDA obligations align with CoreTrustSeal Requirements to some degree, but there is no one-to-one relationship as demonstrated in this report. Achieving TDR status is a big step towards fulfilling the CESSDA obligations, and vice versa, but complying with CoreTrustSeal does not guarantee that the SP adheres to specific CESSDA obligations since CoreTrustSeal is, necessarily, more generic.

From this observation, it follows that the CESSDA SP's will require a common interpretation of the Annex II obligations and what steps they need to take to comply with them. Interpretation and compliance are challenging in a context where so much active work ongoing within CESSDA will have a direct impact on the obligations. This means that it is not possible at this point of time to produce final guidance for the CESSDA SP's on how the deal with the CESSDA obligations in practice. This is why it is recommended that CESSDA provides easily accessible, clear, up-to-date information on each of the Annex II obligations and clear channels of communications about their progress and related activities. In the conclusion of this report (chapter 6) a number of related recommendations is made.

# Abbreviations and Acronyms

| | |
|---|---|
| Annex II | Annex II of the CESSDA Statutes |
| CTS | CoreTrustSeal |
| DIN | Deutsches Institut für Normung (DIN; the German Institute for Standardization) Standard |
| DSA | Data Seal of Approval |
| ICSU | Interdisciplinary Body of the International Council for Science |
| ISO | International Organization for Standardization Standard |
| nestorSeal | nestor Seal for Trustworthy Digital Archives |
| OAIS | Open Archival Information System |
| RDA | Research Data Alliance |
| SP | Service Provider |
| TDR | Trustworthy Digital Repository |
| WDS | World Data System |

# Table of Contents

# 1. Introduction

### Trust and certification

The notion of trust in the repository and other data services offered by CESSDA members is central to their mission of storing, curating, preserving and providing access to data in the long term. Trust is crucial to the archive's relationship with its data depositors and users. National governments indicate trust by designating an organisation at the national 'service provider' (SP) of social science data.

Beyond de facto decisions to trust a service provider, we have the concept of 'trustworthiness' where, by some agreed method, a body indicates that it meets certain criteria which permit them to be trusted. The evolution of standards and processes to apply trustworthy digital repository (TDR) status has met an acknowledged need for standardization and formalization in the area of data repository practice. The ISO 16363:2012 (CCSDS 652.0-R-1) *Audit and certification of trustworthy digital repositories* DIN 31644 *Information and documentation - Criteria for trustworthy digital archives.*, from NESTOR in Germany, and the Data Seal of Approval (now CoreTrustSeal) have provided a number of OAIS-related approaches to certifying trustworthiness.

Successful certification provides a clear, simple to understand, 'badge' of achievement for an organisation, but the benefit of these standards goes beyond providing a clear status mark to the clients and funders of data repositories. The process of developing evidence and agreed practice to support a TDR application generates discussion and conversation across all levels of repository staff, providing a common language for discussing the business of archiving and for considering areas where managed change and improvement are required.

### Trust in CESSDA

In an organisation like CESSDA the adoption of an agreed approach to TDR provides a common perspective on trust across its members. This common understanding of the issues can provide opportunities for cooperation between members, which supports further alignment, improvement and interoperability. Cooperation at the level of process design and documentation can reduce the resource burden of maintaining certification over time.

In 2014 the decision was taken by CESSDA to adopt a common approach to TDR (more on this in the paragraph "CESSDA Adoption of DSA 2014" in chapter 2). In selecting

the DSA (and its successor CoreTrustSeal[1] as the reference TDR requirements CESSDA considered the wider framework of trustworthy digital repository certification (see paragraph CESSDA Adoption in chapter 2) and chose an option which provided the 'core' criteria for governance, infrastructure and digital object management using a low-barrier to entry, peer reviewed approach. The selection of CoreTrustSeal does not preclude members from seeking additional layers of TDR certification and does not conflict with other certification goals (e.g. ISO27001 for Information Security).

The CESSDA approach to delivering TDR is evolving and the process itself allows members to learn more about best practices, about themselves and about each other. Current CESSDA members are not homogenous and they vary greatly in their size, governance, infrastructure, data collections and partnership models. All of these variations mean that local circumstances and practice remain critical, but a common TDR approach allows us to communicate our differences more clearly and leverage our similarities more effectively.

**Trust in the SaW project**

With the SAW project, we have sought Strengthen and Widen participation in the trust mission beyond current membership and into aspiring members and newly created repositories. This engagement and openness is not simply a question of established repositories passing on their expertise to less experienced organisations. Newer repositories with fewer legacy issues and data sets can be more streamlined and more responsive. There is benefit to all sides in the process. In the foreseeable future we expect to deliver and expand our services to meet the new "big data" challenges and the opportunities for research provided by new data sources and data tools. A common approach to trustworthiness provides a lingua franca between CESSDA members to support our continued mission to store, curate, preserve and provide access to data in the long term.

The CESSDA SaW project plan called for the task group to:

Provide support, assistance and monitoring of progress by all SPs towards meeting the TDR requirements and towards certification.

[1] From September 11th 2017, the ICSU World Data System (ICSU-WDS) and the Data Seal of Approval (DSA) are continued as the new certification organisation: *CoreTrustSeal*. In this report, this seal is mostly referred to under its old name DSA, or DSA/WDS, as this was in use almost all the time during the SaW project.

Undertake CESSDA-internal peer-review of self-assessments against the TDR requirements

Map related concepts between the CESSDA *Annex* II obligations and the TDR requirements

In this deliverable, we report on the processes undertaken and the progress achieved in meeting these goals. Chapter 2 provides context by describing prior CESSDA trust activities. Chapter 3 describes the activities of this project while chapter 4 describes the outcomes to date. Chapter 5 considers the TDR requirements alongside the Annex II obligations and chapter 6 presents the conclusions and recommendations. We provide information about the next steps in our journeys towards TDR status in chapter 7. Appendix 1 provides reference information on issues around individual obligations.

# 2. Pre-SaW Trust Activities within CESSDA

The importance of trust and of trustworthiness have long been acknowledged by CESSDA. CESSDA SaW trust works draws on previous trust-related activities within CESSDA. These are described below to provide further context, though due to the differences in participation in SaW and the changes to the TDR criteria (see paragraph "TDR Requirements: from DSA to DSA/WDS") over time, not all of these processes and outcomes are directly comparable.

**CESSDA Trust Workshops - 2013**

The first CESSDA activities to address trust and TDR requirements directly were undertaken in 2013. The processes designed at that time, and the knowledge acquired, continue to inform current work in the SaW project.

Two workshops, with the first taking place in early 2013 in Bergen, brought together a range of current CESSDA SPs and a number of SPs of members which had not yet signed the CESSDA statutes. As both the Statutes and the Trust Criteria cover a range of best and expected practice ranging across governance, digital object management and infrastructure it was decided to combine work in these areas.

As a result of this first workshop an informal working group on trust was put in place including a number of coordinating topic experts with representation from across the existing SPs.

The coordinating topic experts, some with existing experience of the DSA, through self-assessment, certification and through membership of the international DSA Board familiarized themselves with the DSA's core TDR criteria and processes and prepared a cooperative trust process.

The initial activity was to introduce the selected TDR criteria, the Data Seal of Approval (DSA), communicate internally about our interpretation of the criteria and the similarities and differences between our national situations. This provided the common baseline against which we could consider to what degree the SP's fulfilled the requirements of a *Trusted Digital Repository TDR*.

The working group process was in line with that of the Data Seal of Approval Board procedures, self-assessments against the DSA criteria were undertaken by participants. Instead of a formal DSA review process the participants undertook anonymous peer review of each other, ensuring that each repository appreciated the roles of both applicant and reviewer. These reviews and score were then examined by the topic expert group to ensure consistency, including re-scoring against each

requirement as necessary. The explicit purpose was not to criticize individual archives but to provide an overview of their TDR-readiness.

**Output of the workshops: gap analysis**

The key output of these activities was a report and associated *gap analysis* (see chapter 3, under Gap Analysis) based on all the self-assessments and peer reviews across all the SP's. The self-assessments and, especially the gap analysis, were presented and discussed at a second workshop in Cologne in October 2013.

The DSA required the provision of evidence, ideally available on the web, to support each self-assessment statement of compliance against their TDR requirements (this continues with CoreTrustSeal). Where documentation is not available in English, succinct descriptions of the evidence and why it supports compliance is expected. The most notable outcome of the gap analysis was that requirements related to internal repository processes were the least mature. In discussions with participants it was determined that in most cases materials existed where it was necessary to communicate directly with data producers and consumers. Less effort had been expended on formalising *internal documentation* and this translated directly to a lack of evidence for internally focused requirements. Internal processes, especially for smaller organisations, may rely on the knowledge of an individual, and they may not be explicitly documented. In other cases, the review process was made challenging by a lack of English language documentation or English summaries of the existing documentation. The language barrier also presented a challenge to the cross-comparison of evidence which impacted the review process, but is also a barrier to comparability and cooperation between service providers in general.

The gap analysis did not indicate that a lack of particular expertise or infrastructure was a problem for the majority of SPs, though there were weaknesses in the descriptions of the technical infrastructure which might be explained by the more curatorial roles undertaken by those involved with the workshops and self-assessments. Maintenance of the technical infrastructure is often out-sourced, for different reasons and to varying degrees. One of the main outcomes of this process was that most SPs were either in a good position to move towards certification or were aware of the challenges they faced in developing their processes and documentation before an application for TDR status was practical. It was considered that a period of at least one to two years of activity at the local and CESSDA level would be needed before the goal of full CESSDA SP certification could be met.

The process also determined that, while both the DSA and the Annex II obligations related to requirements to be met by SPs, there was limited scope for direct mapping

and common implementation. The underlying theme of discussions regarding Annex II obligations was that further clarification was required on the expectations before much more progress could be made.

**CESSDA Adoption of DSA - 2014**

The CESSDA Work Plan 2014 – 2015 recommended that CESSDA makes certification of its SP's as a TDR mandatory. As the most practical candidate the DSA – Data Seal of Approval was proposed. This recommendation was based on the Trust activities described above and the fact that the DSA had already seen adoption among members with some having acquired certification and others with self-assessments in progress.

The selection of the DSA as the primary vehicle for TDR certification within CESSDA was based on it being a low-barrier to entry lightweight (core), certification mechanism. The sixteen DSA requirements for Trustworthy Digital Repositories, related to, respectively, Data Producers, Data Repositories and Data Consumers. The certification process consists of self-assessment followed by a peer review process, both enabled by an online tool. Both standard and process were overseen by an international board. There is no site visit or audit (in contrast to ISO 16363 certification). The DSA was granted for a period of two years.

The other certification standards on long term preservation, DIN 31644/nestorSeal or ISO 16363, were considered to be too heavyweight, too complicated, and/or too immature (ISO16363 was still a candidate standard at the time) and possibly too expensive to use. The CESSDA TDR approach, including expansion to alternate standards may change in future.

Other reasons mentioned for making the TDR certification mandatory were:

- To instil trust between the SP's, one of the goals of CESSDA.
- Future funding might depend on it: increasingly funding bodies might make a TDR status mandatory for data curation / data preservation.
- It gives clarity of evidence and terminology within CESSDA. This could be of importance for the interpretation of the Annex II Obligations.

This recommendation was adopted unanimously by the General Assembly in June 2014 and the goals of achieving Trusted Digital Repository status through the DSA and of meeting the obligations in Annex II were initially set a target of being delivered by the end of 2015. However, the working group did not convene until the end of 2015 and the further activities to clarify the Annex II obligations were not undertaken at that time. The activities of the Trust Working Group (further: Trust Group) were resumed at the CESSDA Expert Seminar late in 2015 (see the next chapter).

**TDR Requirements: from DSA to DSA/WDS - CoreTrustSeal**

By 2013 the Data Seal of Approval had moved out of the originators (DANS) and was being managed by an international board. The wording of the requirements had already been slightly changed to focus more generally on data, rather than solely 'research data' but the DSA community remained predominantly repositories handling research data in the social sciences and humanities. By this time, the World Data System (WDS) of ICSU had developed membership criteria which included extensive TDR elements. It was considered that the provision of a single 'core' TDR certification approach was better for the data management community as a whole and between 2014 and 2016 the DSA and WDS reviewed their goals, processes and procedures in the context of a Research Data Alliance (RDA) working group. Group members came primarily from the DSA Board and WDS Membership Committee but participation was open and progress reports were provided to the wide-ranging membership of the Repository Certification Interest Group. The group released a set of common requirements and common procedures for public comment and undertook internal testing (by both WDS and DSA members) of the revised requirements.

After a long open comment period, the new criteria were adopted by both DSA and WDS in 2016.

There were still 16 requirements, though their structure and content had changed to provide clearer language and a greater alignment with the other TDR Framework standards.

There were changes to the structure of the requirements: six on organisational infrastructure, eight on digital object management and two on technology. Extensive care was taken to ensure consistency between the old and new approaches such that prior WDS or DSA recipients would be able to renew to the new requirements. However, the requirements are not identical with more detail provided on documented public evidence requirements and a greater focus on technical infrastructure and appropriate information security.

During the self-assessment, each applicant indicates a compliance level for each of the requirements:

0 – Not applicable
1 – The repository has not considered this yet
2 – The repository has a theoretical concept
3 – The repository is in the implementation phase
4 – The guideline has been fully implemented in the repository

The compliance levels provided by the applicants will be judged against the given evidence by the reviewers.

As of August 2017, the two bodies constituted an interim DSA-WDS Board to manage the process and requirements. A new common tool and a new CoreTrustSeal brand to support a new independent board will replace the interim board when statues and business model considerations are agreed.

While the transition of the requirements has been designed to minimize impact on any single applicant there is of course an impact on the CESSDA activities. SaW trust work has adopted the new common requirements, making it impossible to directly compare the current status with that at the time of the 2013 workshops. For SPs which were already in the process of developing self-assessment it has been necessary to revise their work to align with these new requirements. The Trust Group is still in the process of assimilating the new requirements and evidence requirements and firm guidance will only be possible in some areas once a critical mass of repositories have been certified against the common TDR standard.

# 3. CESSDA SAW trust activities

In line with task 4.3 of the CESSDA SaW project plan ("Development Support: achieving the Data Seal of Approval") the Trust Group undertook a process which closely paralleled that of the initial 2013 activities, though with a different and larger range of participants and against the new (and at the time evolving) 'core common TDR requirements' which became the CoreTrustSeal.

The activities of the Trust Group during the CESSDA SaW project were preceded by the CESSDA Expert Seminar 2015. The timing of this seminar made it possible that its discussions and conclusions could feed into the CESSDA SaW project, starting around the same time. During the SaW project two workshops were organised. At the first in in June 2016 in The Hague, the concepts of trust and certification were (re-)introduced to all the new larger group of SP's. In the second workshop, in March 2017 in Zagreb, a new gap analysis based on all the self-assessments submitted by the SP's was presented. These self-assessments were peer reviewed and analysed by the Trust Group (being the task group 4.3 of CESSDA SaW). For a full report of the expert seminar and the two workshops see deliverable D4.1, the "Trust" Workshop report and the Milestones MS19 "Evaluation of already existing ideas and plans" and MS20 "Proposal on how to set up the Trust Group".

# 4. Service Providers' progress with respect to DSA certification

In December 2015, at the time of the CESSDA Expert Seminar, five CESSDA Service Providers had acquired the DSA certification: UKDA, DANS, GESIS, FSD and NSD, slightly later followed, in 2016 by CSDA and SND. This was the DSA certification for the 2014-2017 period. In addition, some SPs reported being very close to acquiring DSA.

Half a year later, at the workshop in The Hague (June 2016), the number of certified SP's had not increased: seven SP's had reached certification or were nearly there. Six other SP's were still somewhere in the process of writing up their self-assessment, either just starting or in a more advanced stage, but had not yet submitted. Nine other SP's were not even in that phase; they simply were not yet established or in one way or another unclear about their status. In short, it was for these nine SP's not yet possible to fill in essential parts of the self-assessment (mission, technical infrastructure etc.).

**Testing the self-assessments**

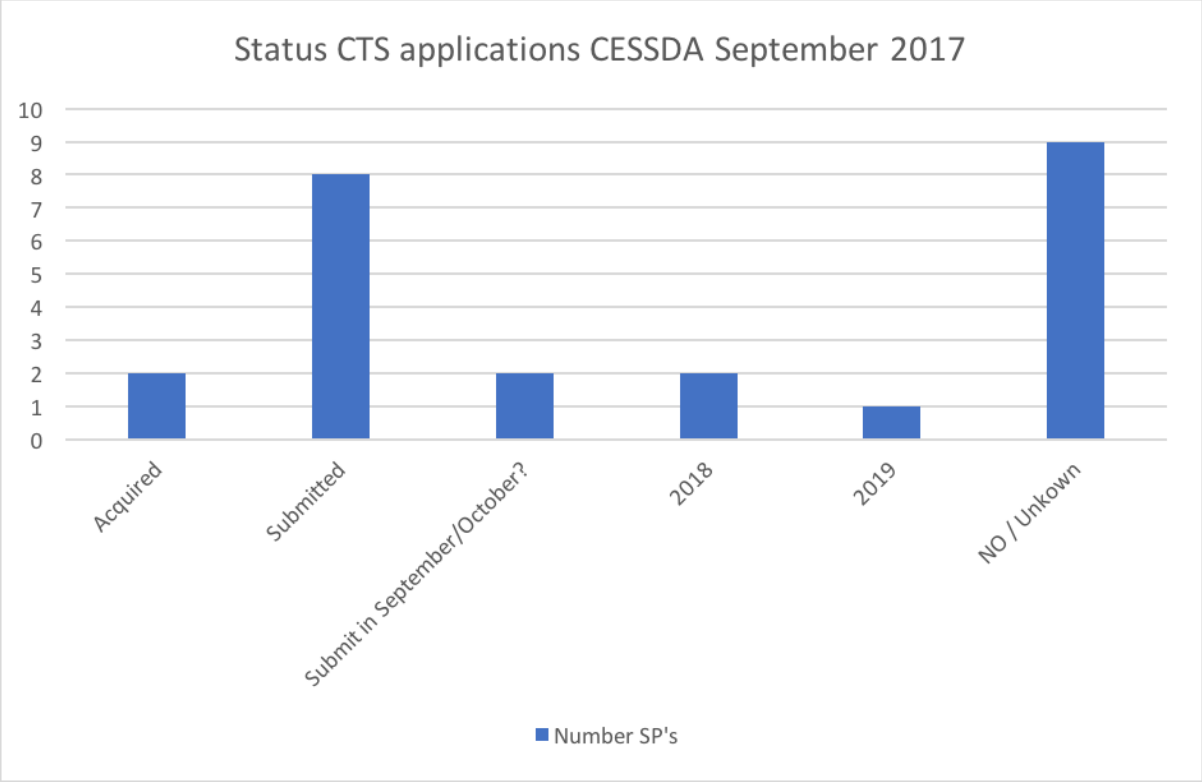
In March 2017, at the time of the Zagreb workshop, the situation had changed as the new DSA-WDS CoreTrustSeal requirement had been released. This means that at that time no self-assessments were submitted. All SP's, old or new, had to re-submit a self-assessment to be certified according to the new requirements. This change also means that the figures are not comparable between June 2016 and March 2017. However, responding to the call of the Trust Group, all in all 15 self-assessments were sent to the Trust Group for feedback, out of the 23 SP's. This enabled a gap analysis of which the results are detailed in deliverable D4.1.

In the table below the final results are shown as of September 2017. The total score is that two seals have already been acquired, eight self-assessments have been submitted effectively for review by the DSA/WDS Board and another five have announced to do that "soon", meaning either in 2017 or 2018. For another nine SP's this is however as yet impossible, mainly due to the reasons mentioned earlier: uncertainty about their formal organisational status, in particular of umbrella organisations being in the middle of a reorganisation, no guaranteed funding for any period longer than one or two years, etc.

*Table 1: Status CoreTrustSeal applications September **2017***

| Status CoreTrustSeal - September 2017 | |
|---|---|
| Acquired | 2 |
| Submitted | 8 |
| To submit in 2017 | 2 |
| To submit in 2018 / 2019 | 3 |
| No plans yet / unknown | 9 |
| Total | 24 |

*Figure 1 Status CoreTrustSeal applications CESSDA September 2017*




**Analysing the final result**

For analysing the final figures (table 2) we can divide the SP's in two groups. On the one hand, there are the SP's that have, as of September 2017, already acquired CoreTrustSeal-certification status (2), are in the process of being reviewed by the CoreTrustSeal Board (8) and those who have announced to do that "soon", meaning either in 2017 or 2018 (5). Of this latter category ("submitting soon"), we cannot be

completely sure of course (promising is not the same as doing), but most of these promised submissions seem to be rather safe, based on the quality of their self-assessment sent in as test in February /March 2017. This group totals 15 SP's. Most in the group of ten SP's having submitted and/or acquired the CoreTrustSeal, were already earlier DSA-certified. From these figures, it follows that there is an increase in SP's complying with the certification seal, now or soon to come. On the other hand, there is the group SP's who will *not* submit a self-assessment in the near future, in most, but not all, cases because they are not able to do so yet: 9 SP's.

The first group consists of the SP's of eleven members and of four (aspiring) partners[2]. The second group consists of the SP's of four members and of five (aspiring) partners. Most of the SP's in the first group, and certainly the SP's who have effectively submitted ultimately September 2017, can be characterised as being longer in existence than the average CESSDA SP. Consequently, they mostly have a larger staff. They are, as a rule, certainly older than the SP's in the second group, whether member or partner, with one or two exceptions. The distinction member versus (aspiring) partner should not be taken too strictly as for formal, political, reasons some partners are (not yet) member officially while already being an established repository. An example is the position the acquired certification of the FSD, while Finland is not yet a formal member of CESSDA.

Looking from a more critical point of view it could be said that is it worrying that out of the fifteen existing ***members*** only eight have actually submitted their self-assessment, another three have the intention of doing so in this year or in 2018/2019 and that another four either have indicated nothing or told us not be able to submit self-assessments in the near future. Some of the members in this latter group have absolutely good and legitimate reasons for not being able yet to send a self-assessment, like major reorganisations or repositioning operations of themselves or in the overarching organisations, but for others this is not always clear. In other words, being a member is not a guarantee of submitting soon a self-assessment. Some ***partners***, clearly seem to be in a better position than others to reach the stage of the submission of a self-assessment.

For nine SP's, either member or partner, submitting is as yet impossible, mainly due for the reasons mentioned earlier. For existing SP's there may be uncertainty about changes in their formal organisational status, funding etc. For most of the partners, in particular newcomer SP's, it has become clear that preparing a full self-assessment is

[2] Partners or observers: those service providers whose countries have not yet reached the official status of being a member of CESSDA.

for several reasons not something which is carried out overnight, if not virtually impossible to do in the first years of their existence. These new SP's might have constitutional and organisational uncertainty for a longer period of time, in particular uncertainty on funding for the next three to five years.

**Conclusions: major hurdles in achieving certification**

Even if continuity would be guaranteed for at least a medium term (three to five years) then fulfilling all the requirements is still quite a heavy task for starters. The gap analysis presented March 2017 exposed very clearly that lack of proper evidence (missing documentation on technical infrastructure, workflows, preservation policies and plans etc.) produced the lowest compliance *levels on average*. Starters, in particular small starters, have to set up all this documentation from scratch. The scale of the new or not yet founded SP's is simply too small to run a professional repository at the start. In particular the emphasis in the CoreTrustSeal-certification on producing as much evidence as possible, also preferably publicly available and in English, is much demanding from a small-staffed starting repository. Technical infrastructure is also often not fully functioning and certainly not thoroughly documented. All this is less of a problem for those members, which exist for a longer period and are in a stable position.

# 5. CESSDA Annex II Obligations and the DSA guidelines

The Statutes for CESSDA includes fourteen Annex II Obligations[3] that must be met by SPs. The seventh Obligation is that SPs shall adhere to the principles of the OAIS reference model and any agreed CESSDA ERIC requirements for operating trusted repositories. CESSDA has agreed that the SPs need to acquire the CoreTrustSeal Certification to demonstrate that they are a Trustworthy Digital Repository.

Many of the CESSDA Obligations are parallel to the DSA Requirements[4] but there are no one-to-one relationships. In this chapter, we examine how the CESSDA Obligations and the DSA Requirements are related, and discuss how the Obligations could be clarified, defined and translated into a more workable criteria and goals for SPs.

**The Annex II Obligations**

1. CESSDA Service Providers shall:
2. be compliant with the agreed elements of the DDI metadata standard that are required to enable the member/observer to contribute to CESSDA ERIC activities and which will be identified by CESSDA ERIC;
3. adopt and apply the common single sign-on user authentication system(s) recommended by CESSDA;
4. enable the harvesting of their resource discovery metadata and relevant additional metadata for inclusion in the CESSDA ERIC data portal;
5. make their data holdings downloadable through common data gateways as far as permitted by the relevant legislation and regulations;
6. ensure that the applicable national language(s) within the multi-lingual thesaurus are maintained;
7. share their data archiving tools (under the Intellectual Property conditions described in Article 11 of the Statutes);
8. adhere to the principles of the OAIS reference model and any agreed CESSDA ERIC requirements for operating trusted repositories;
9. contribute to CESSDA ERIC's cross national data harmonisation activities;
10. contribute material and/or expertise to the cross-national question bank;
11. provide mentor support for CESSDA ERIC Observers and their representative Service Providers to achieve full Membership;

[3] CESSDA ERIC Statutes. https://www.cessda.eu/content/download/1466/20924/file/STATUTES%20of%20CESSDA%20ERIC_2017.pdf

[4] WDS/DSA: the Core Trustworthy Data Repository Requirements: https://www.datasealofapproval.org/en/information/requirements/

12. provide member support for countries with immature and fragile national infrastructures to help them build up needed competence later to be able to fulfil tasks as Members;
13. facilitate access to national government and research funded relevant data, dependent on national legal systems;
14. adhere to CESSDA ERIC's Data Access and Dissemination Policies;
15. adhere to the provisions of the Organisation's policies as required.

**CoreTrustSeal Requirements**

The CoreTrustSeal Requirements cover organizational infrastructure, digital object management, and technology.

1. The repository has an explicit mission to provide access to and preserve data in its domain.
2. The repository maintains all applicable licenses covering data access and use and monitors compliance.
3. The repository has a continuity plan to ensure ongoing access to and preservation of its holdings.
4. The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.
5. The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.
6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either in-house, or external, including scientific guidance, if relevant).
7. The repository guarantees the integrity and authenticity of the data.
8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.
9. The repository applies documented processes and procedures in managing archival storage of the data.
10. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.
11. The repository has appropriate expertise to address technical data and metadata quality and ensures that sufficient information is available for end users to make quality-related evaluations.
12. Archiving takes place according to defined workflows from ingest to dissemination.

13. The repository enables users to discover the data and refer to them in a persistent way through proper citation.
14. The repository enables reuse of the data over time, ensuring that appropriate metadata are available to support the understanding and use of the data.
15. The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.
16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.

**Relationship between CESSDA Obligations and CoreTrustSeal Requirements**

As stated earlier, there is no one-to-one relationship between individual Obligations and the CoreTrustSeal Requirements. However, there are some partial relationships between these two sets of criteria so meeting the Requirements will mean taking steps towards fulfilling the CESSDA Obligations, and vice versa. The relationships are outlined broadly in table 2 below.

*Table 2: Relationships CESSDA Annex II obligations – DSA requirements*

| | | DSA Requirements | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CESSDA Statutes** | | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** |
| 1 | compliant with the agreed DDI elements | | | | | | | ■ | ■ | | | ■ | | ■ | ■ | | |
| 2 | common single sign-on | | ■ | | | | | ■ | | | | | | | | | |
| 3 | harvesting of metadata | | | | | | | | | | | ■ | | ■ | | | |
| 4 | data holdings downloadable through common data gateways | | | | | | | | | | | | | | ■ | | |
| 5 | national languages within thesaurus | | | | | | | | | | | | | ■ | | | |
| 6 | share data archiving tools | | | | | | ■ | | | | | | | | | ■ | |
| 7 | requirements for trusted repositories | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| 8 | contribute to cross national data harmonisation | | | | | | | | | | | | | | ■ | | |
| 9 | contribute to cross-national question bank | | | | | | | | | | | | | ■ | | | |
| 10 | mentor support for Observers | | | | | | | | | | | | | | | | |
| 11 | mentor support for countries with immature infrastructures | | | | | | | | | | | | | | | | |
| 12 | facilitate access to national relevant data | | | | | | | | | | | | | ■ | | | |
| 13 | adhere to Data Access and Dissemination Policies | | ■ | | | | | | | | | | | ■ | ■ | | |
| 14 | adhere to other policies | | | | | | | | | | | | | | | | |

The only Obligation that fully matches the CoreTrustSeal Requirements is Obligation 7: *Service Providers need to adhere to the principles of the OAIS reference model and any agreed CESSDA ERIC requirements for operating trusted repositories.* This is self-evident since CESSDA's requirement for operating trusted repositories is CoreTrustSeal.

Most CESSDA Obligations are about data and metadata discovery, access, and enabling reuse of data and metadata. If Service Providers adhere to the Obligations, they are likely to adhere to the CoreTrustSeal Requirements on data discovery and reuse. On the other hand, holding the CoreTrustSeal does not guarantee that the SP adheres to specific CESSDA Obligations since CoreTrustSeal is more generic than the Obligations.

Thus, Obligations need to be further specified in operational criteria that are clear from the point of CESSDA-specific implementation requirements and are measurable from the point of fulfilment of those requirements. This is elaborated in the next chapter as recommendations.

Obligations 10, 11 and 14 are not directly related to any CoreTrustSeal Requirements. However, the availability of consistent, comparable public evidence for the CoreTrustSeal across Service Providers can be considered as mentor support and at least will help provide this support.

**Turning Annex II Obligations into workable goals for SPs**

There is still a lot of confusion about the Obligations among the Service Providers. The main questions are related to how SPs can comply with the Obligations, how they can show that they are compliant, and what the timetable is. Thus, CESSDA needs to turn the Obligations into workable goals. Since CESSDA is currently in an active service building phase, for some Obligations this work has already started and even finished, for others not.

The Trust Group has charted SPs questions and opinions about the Obligations. Many of the questions asked by the SPs during the SaW project and before have already been answered, or will be answered in 2017-2018. In the table below, we have summarised all remaining questions at the time of writing (September 2017).

All questions about Obligations, and some answers, are provided in Appendix 1. They reflect well what kind of information SPs need during all improvement and development processes.

**Issues of Individual Obligations**

Table 3 summarises SPs' main questions about each Obligation (at the time of writing September 2017).

*Table 3: Questions of SP's on the Annex II obligations*

| | **Obligation: CESSDA SPs shall…** | **Questions/comments from the SPs** |
|---|---|---|
| 1. | be compliant with the agreed elements of the DDI metadata standard that are required to enable the member/observer to contribute to CESSDA ERIC activities and which will be identified by CESSDA ERIC; | What are the activities (services) where metadata are needed?<br>In which languages should the metadata be?<br>What is the deadline for SPs to produce required metadata? |
| 2. | adopt and apply the common single sign-on user authentication system(s) recommended by CESSDA; | What is the common single sign-on ?<br>Which resources or services should be accessible via single sign-on? When? |
| 3. | enable the harvesting of their resource discovery metadata and relevant additional metadata for inclusion in the CESSDA ERIC data portal; | How do various CESSDA components (like OSMH, CMM, PaSC) work together and how do metadata "flow" between systems? |
| 4. | make their data holdings downloadable through common data gateways as far as permitted by the relevant legislation and regulations; | What are the (main) services CESSDA aims to offer?<br>Which data holdings should be accessible or downloadable via CESSDA? In which formats and under which condition? |
| 5. | ensure that the applicable national language(s) within the multi-lingual thesaurus are maintained; | Ongoing projects like CV Manager and CMM2, will address this obligation and undoubtedly rise questions. |
| 6. | share their data archiving tools (under the Intellectual Property conditions described in Article 11 of the Statutes); | Will the forthcoming policies for software and tools adoption answer questions about sharing data archiving tools?<br>What costs and fees are included here? |
| 7. | adhere to the principles of the OAIS reference model and any agreed CESSDA ERIC requirements for operating trusted repositories; | |
| 8. | contribute to CESSDA ERIC's cross national data harmonisation activities; | What are CESSDA's expectations?<br>Is there a central reference point for these activities? |
| 9. | contribute material and/or expertise to the cross-national question bank; | What roles should or will the SPs have here? |
| 10. | provide mentor support for CESSDA ERIC | In what form should this support |

| | | |
|---|---|---|
| | Observers and their representative Service Providers to achieve full Membership; | be?<br>How are the support activities organised and monitored?<br>What would be the degree of central management? |
| 11. | provide member support for countries with immature and fragile national infrastructures to help them build up needed competence later to be able to fulfil tasks as Members; | Should this be read as 'mentor support' like 10 above or does this refer specifically to full members providing support to others outside CESSDA?<br>In what form should this support be?<br>How are the support activities organised and monitored?<br>What would be the degree of central management? |
| 12. | facilitate access to national government and research funded relevant data, dependent on national legal systems; | What is expected from SPs?<br>How SPs can show that they adhere to this Obligation? |
| 13. | adhere to CESSDA ERIC's Data Access and Dissemination Policies; | - |
| 14. | adhere to the provisions of the Organisation's policies as required. | - |

All in all, CESSDA should clarify and define for each Obligation:

- Responsible Working Group ("Owner of Obligation"; could be the Main Office, too)
- Related Work Plan Project(s)
- Related other Projects
- Metrics (how compliance with Obligation is measured)
- Timeline
- Costs for SPs

**Recommendations Annex II**

The Trust Group has formulated the following recommendations:

1. Service Providers need on-going and up-to-date information about CESSDAs Work Plan Task and possible other projects and their progress, and about progress regarding the obligations, their operationalisation and implementation. This information should be available at one central point at CESSDA, internally for example in a Basecamp map.
2. This means that for each obligation, it needs to be clearly identified whether there is current or planned activity to refine or support reaching the goals and which groups and/or processes are supporting that process (see for a start

Appendix 1 of this deliverable). It is the responsibility of the Main Office to oversee this and, in particular to take care of existing gaps.

3. It should also be clear what parts of the obligations are established "official" CESSDA policy (like the Data Access Policy) and which ones are still under consideration (like the metadata policy at the moment).
4. Clarity is needed on what the common CESSDA Services will be in the future, and what are the professional standards aimed at.
5. For many obligations decisions on a (CESSDA-) political level are needed followed by an implementation guide on how to implement these.
6. Step-by-step implementation might be best for several obligations. Service Providers need timelines and deadlines (a roadmap), and in many cases also cost estimations.
7. The different position and context of Service Providers should be taken in consideration as some Service Providers are fully established and others just begin to build up.
8. Service Providers need training on best practices regarding the obligations.
9. CESSDA needs to monitor how SPs comply with obligations with a clear and transparent system and metrics.

# 6. Conclusions drawn from the CESSDA SaW project[5]

Task 4.3 of the SaW project had, basically, two separate aims:

1. Provide support, assistance and monitoring of progress by all SPs towards meeting the CoreTrustSeal requirements and towards certification, by undertaking CESSDA-internal peer-review of self-assessments against the CoreTrustSeal requirements
2. Map related concepts between the CESSDA Annex II obligations and the CoreTrustSeal requirements

In this chapter, the main conclusions of task 4.3 of the SaW-project are presented, as well as a number of recommendations for CESSDA.

**Certification**

The first task was directed at the certification of all SP's as trustworthy digital repositories, made mandatory in 2014 by CESSDA. The SaW project has enabled the trust expert group which was informally established in 2013 and now being the project team of task 4.3, to take up again the issue of certification, this time on a larger scale. The sequence of having the expert seminar in December 2015, followed by the two workshops in June 2016 and March 2017 ensured knowledge about and engagement with TDR issues. During the project period, most SP's either started or continued their work on certification leading to a number of self-assessments effectively submitted to the CoreTrustSeal Board and/or significant progress towards that goal.

In other words: much has been achieved during the course of the project. The same approach was followed as in 2013. The cooperation with and between all SP's and in particular the system of reviewing test self-assessments proved fruitful again. Discussing the requirements of the CoreTrustSeal, presenting a gap analysis, but also the intense consultancy on a one-to-one basis as offered in the Zagreb Workshop (March 2017) were all valuable elements in helping the SP's achieving their certification or at least to raise awareness. Communication and cooperation with all the SP's was supported by the formation of a group of contact persons within each SP working together with the 4.3 task group. The activities of the latter will be continued in 2018 as a Trust group in CESSDA. The formation of this TDR contact group is also an important element for continuity after the end of the project.

[5] In this paragraph the DSA/WDS seal is referred to as CoreTrustSeal CTS, as this paragraph mostly deals with present and future developments.

To ***summarise*** the points mentioned: It was the intention of the SaW-project to have as many repositories certified as possible. For some of the reasons mentioned in the previous paragraph this was still an impossible hurdle to take for a number of SP's, certainly in the time frame of the SaW-project. A special challenge for all was the switch from the DSA to the CoreTrustSeal certification during the course of the project (early 2017). However, despite the transitional challenge of changes in the requirement this part of the project can be evaluated in an optimistic way: more than half of the CESSDA SP's have either almost reached certification or can reasonably be expected do so within a little bit more than a year. Of the ten SP's who have not achieved this it can be said that most of them are starting and, consequently, will not be able do that soon. So, the mandatory obligation of certification is for CESSDA for some years to come a continuous task.

The whole process will need further guidance and consultancy by the Trust group. For 2018 this is foreseen in the Working Plan for CESSDA (see paragraph 7). The activities in 2018 will be directed both at newcomers under the SP's and at those already on course leading those towards certification.

**Recommendation for CESSDA Trust Certification**

A general consideration, when looking at the figures presented here, is that the main problem SP's have are either lack of sustainable funding or unclearness of their organisational embedding. CESSDA should be clear in what period of time certification should be achieved by a SP. By pointing to the impossibility of achieving certification, the SP concerned could convince their ministry and/or research council/academy in getting extra funding or a better organisational place. This would mean that CESSDA anyway should monitor at regular intervals the status of all SP's regarding certification, in the same way compliance with Annex II obligations should be monitored (see next paragraph).

**Annex II obligations**

Many of the CESSDA obligations concur with the mandatory Core Trust Seal (formerly DSA) Requirements but there are no one-to-one relationships. As observed in the previous paragraphs meeting the CoreTrustSeal Requirements will mean taking steps towards fulfilling the CESSDA obligations, and vice versa. On the other hand, complying with the CoreTrustSeal does not guarantee that the SP adheres to specific CESSDA obligations since CoreTrustSeal is more generic than the obligations.

It follows from this observation that, regardless of achieving CoreTrustSeal certification, the CESSDA SP's will have to know how to interpret the Annex II obligations and what they are required to do.

There is a lot of work going on now in a number of working groups and project groups within CESSDA. Much of this work has direct implications for the obligations. This means that it is not possible at this point of time to produce final requirements and/or guidelines for the CESSDA SP's on how the deal with the CESSDA obligations in practice.

**Recommendations Annex II obligations**

This leads to the general recommendation to CESSDA that transparency is vital in order to avoid a general state of confusion among the Service Providers.

There has to be a clear channel of communication, internally, maybe also externally, where for each obligation the up-to-date status can be found. For some obligations, this information might be a "definitive" guideline, for other obligations however this still might be "work in progress" for some time to come. Anyway, it should be clear to the SP's at all times which obligations, or parts of these, are established, "official", CESSDA policy (like the Data Access Policy) and which ones are still under consideration (like the Metadata Policy).

A channel for communication is necessary, at least for the time being, However, when all the obligations contain finalised and clear guidelines/requirements, this should become a permanent tool within CESSDA. The tool would contain, in other words, the operationalisation of the Annex II obligations. It could be updated as much as necessary (not too often). This would keep the Annex II text as stable as possible and would prevent more cumbersome renewal of the Annex II itself. This does not alter the fact that the text of the Annex II should not be seen as untouchable. Some obligations are referring to an outdated state of technology. In Appendix 1 of this report we have summed up a number of critical questions concerning the Annex II obligations.

What the task group would recommend, practically speaking, is to set up this tool as a collection of operational goals, with time schedules and delivery methods attached. Monitoring how SPs comply with the obligations with a clear and transparent system and metrics should be considered. It should contain information on the following points:

- Responsible Working Group

- Related Work Plan project(s)
- Related other project(s)
- Timeline
- Metrics
- Costs

These general considerations have been elaborated in a detailed list of recommendations, to be found at the end of chapter 5.

# 7. Activities Trust Work Plan Group after the CESSDA SaW project: Plan

The work plan is laid down in the proposal for the budget 2018 of the Trust group, approved by the General Assembly of CESSDA, June 2017. Main element is a round of two workshops for an assessment test procedure, during which self-assessments are reviewed and discussed with SP's, leading to an increase in certified SP's. The concrete goals are:

1. 1.(Q1) Introductory workshop for SP's first time in certification (optionally for older ones as well)
2. (Q2) Reviewing self-assessments by the Trust Group
3. (Q4) Second workshop discussing results reviews

Besides these goals the Trust group should anyway continue its cooperation with all the SP's on trust issues, in particular certification. Keeping in contact with the trust contact persons is an essential condition for that and enables the provision of consultancy on an "individual" SP level. Imposing time schedules, as recommended, would give the Trust Group the opportunity to monitor progress more closely.

The Trust Group could also play a role in constructing and maintaining a clear channel of communication on the Annex II obligations, as recommended (see Appendix 1 for a begin). Also monitoring compliance with the obligations by the SP's could be carried out by the Task Group, possibly in some cooperation with the Main Office.

# List of tables



# List of figures

# Appendix 1. Issues about Individual Obligations

**1. Be compliant with the agreed elements of the DDI metadata standard that are required to enable the member/observer to contribute to CESSDA ERIC activities and which will be identified by CESSDA ERIC;**

Questions from the Service Providers:

- Which DDI standard? Codebook or Lifecycle? Which elements are mandatory and which recommended?
- How is compliance defined? Compliant database models for storage vs. the ability to export in acceptable formats vs. the ability to make those formats available for harvesting.
- How much effort/cost is this for a repository?
- An impact analysis should be made.

These questions will be at least partly answered when the Product and Service Catalogue will be published by the end of 2017. The CMM project released a CESSDA Metadata Portfolio in May 2017 and the metadata work continues in a Phase 2 project. CMM work includes an impact analysis. The CESSDA Open Source Metadata Harvester (OSMH) has produced a metadata harvester.

The remaining questions are related to metadata policies and forthcoming services:

- In which language(s) should the metadata be?
- What are the activities or services that require metadata? Product and Service Catalogue, Euro Question Bank, …?
- What is the deadline for SPs to produce the required metadata for each activity/service?

**2. Adopt and apply the common single sign-on user authentication system(s) recommended by CESSDA**

Questions from the Service Providers:

- What this will be, when will it exist, how soon it must be adopted, and what the licencing implications will be?
- Do we have an awareness of the current status of national sign-on systems and the implications of integration?
- What is the relationship to CESSDA's Data Access and Dissemination Policy?

All in all, it seems to be unclear how far this has progressed within CESSDA and within other ERICs. CESSDA Data Access Policy (June 2016) does not state anything about single sign-on. Service Providers need tangible information about what is the common SSO and which resources or services should be accessible via SSO and when.

**3. Enable the harvesting of their resource discovery metadata and relevant additional metadata for inclusion in the CESSDA ERIC data portal**
Questions from the Service Providers:

- Is all of the resource discovery metadata a subset of the DDI?
- Relationship with the technical working group and the metadata group?
- Common minimal standard of versioning for CESSDA?

This Obligation is closely related to Obligation 1. The CMM 1.0 metadata includes resource discovery metadata, and PaSC and CMM are working together on a PaSC metadata profile. The Open Source metadata harvester (OSMH) is a tool built for harvesting. However, it seems to be unclear to the SPs how all these components work together and how metadata will "flow" from their own systems to CESSDA systems.

The CESSDA PID Policy states that "CESSDA SP should implement a version control and assign a new PID to each new version of a dataset" and gives some examples.

The Obligation mentions "relevant additional metadata". The CESSDA Trust group recommended paying particular attention to the definition, collection and management of preservation metadata since knowledge about and use of preservation metadata seemed to be not widespread within the CESSDA community. All in all, "relevant additional metadata" is dependent on the services and products CESSDA aims to offer to the research community (see also Obligation 1).

**4. Make their data holdings downloadable through common data gateways as far as permitted by the relevant legislation and regulations**
Questions from the Service Providers:

- Does this apply to redirect from the CESSDA portal or to provision of access in response to requests from other data gateways?
- Is there a persistent identifier approach which will underpin such a system?
- Legal problems may arise if/when data are downloaded internationally.
- How are the access requests handled?
- Relationship to CESSDA's Data Access and Dissemination Policy?
- Clear dependency on single sign-on, access criteria and technical issues.
- Definition of the concept 'downloadable' within the organizational and technical CESSDA context: Which data in which condition?
- Needed: best practice recommendations with regard to condition of data (e.g. data formats, preparation standards).

All in all, this Obligation seems to be confusing to the Service Providers. Some questions are answered by the CESSDA PID Policy and Data Access Policy but clearly this is an Obligation that needs further elaboration and is related to several other Obligations and solutions. The main questions here are related to what services

CESSDA aims to offer, and which data holdings should be accessible or downloadable via CESSDA portal.

**5. ensure that the applicable national language(s) within the multi-lingual thesaurus are maintained**

Questions from the Service Providers:

- This is about the ELSST thesaurus. How about common controlled vocabularies?
- What proportion of ELSST has to be translated?
- What are the local languages to be used in the multi-lingual thesaurus? Dutch, for example, is not maintained in ELSST at the moment ('local language' is not the same as 'national language' in the case of DANS for the Netherlands).
- What costs are involved?
- ELSST licensing terms and IPR needs to be solved.
- Maintenance and management tool needed.

A 2017 Work Plan Task Project, the CV Manager project, will address many of these questions. For Work Plan 2018, a proposal has been submitted about the Vocabulary Services Multilingual Content Management Phase. In addition, one of the tasks in the CMM Phase 2 project is to produce a maintenance and management plan for the core metadata model and the CVs. The WPT Projects will undoubtedly rise more precise practical and policy questions that need to be addressed appropriately.

**6. share their data archiving tools (under the Intellectual Property conditions described in Article 11 of the Statutes)**

Questions from the Service Providers:

- Should this sharing be done under Open Source conditions? Are all SP's up to that?
- Are fees needed to meet possible costs or will CESSDA fund this?
- Article 11 is on the legal IP aspects. Could this point be clarified by the CESSDA BoD or GA?
- What are the implications for tools built on top of proprietary systems or those built using project funding with conflicting terms for sharing/IP?
- ELSST can be seen as a data archiving tool - the ELSST licence issue needs to be clarified.
- What about tools that may provide a revenue stream to the originating archive from outside of CESSDA? E.g., a software solution that the originating archive could sell as a service to some third party. Sharing the software as open source will make monetizing it difficult as anybody could set up the service.
- Relevant tools need to be identified and standardised information about them compiled and made available to all SPs.

CESSDA's Technical Working Group is creating policies for software and tools adoption that will probably answer some of these questions. ELSST licence issue is

related to Obligation 6, too. It is worth noting that costs and fees are mentioned more frequently here than in questions about other Obligations.

This Obligation is also related to CESSDA's Strategic Aim 3: Maintain a technical development programme to support the work of the CESSDA ERIC, its members and collaborators. In Theme 3.3, common tool kit is referred and Sub-Theme 3.3.1 mentions "Support and foster the development of modular common tool kit to be used internally by data organisations linked to the CESSDA ERIC, including: multi-lingual thesaurus management tools; data 'publishing', ingest processing tools; data access, dissemination, browsing and visualization".

Provision of tools or collaboration in their production can be considered as cost effective for individual SP. Examples include the SaW Task 4.4 Development Support: Establishing the necessary conditions for creating new or reinforcing existing social science data services.

The activities that can be used further in the Obligation 6 specification, are:
a. Establish the demand for development support services (also on the basis of 3.2)
b. Establish the supply of development support services
c. Pilot of delivery of development support services on the basis of a. and b.
d. Develop a sustainability model for development support services
e. Funding models and identifying funding opportunities / possible sources of finance

Common (software) tools provision can be also considered as a support activity for most other Obligations fulfilment and should be planned accordingly on the level of each of Obligations.

**7. adhere to the principles of the OAIS reference model and any agreed CESSDA ERIC requirements for operating trusted repositories**
Questions from the Service Providers:

- Is this covered by the DSA certification? Yes, we believe it is - but where has it been stated?
- What are the costs of acquiring certification?

It has been decided that acquiring the DSA certification is mandatory for Service Providers.

Task 4.3 is supporting Service Providers in their trust process. The current DSA-WDS certification is free, but it is expected that part of the new CoreTrustSeal business model will include a service fee. The cost of DSA for each SP depends a lot on their starting point. If they have documented processes and procedures in place for ingest, preservation, data management and access, submitting a DSA application will require

only couple of hours' work. On the other hand, if relevant documents and required evidence are missing, the process can take several person months.

**8. contribute to CESSDA ERIC's cross national data harmonisation activities**
Questions from the Service Providers:

- How far should data harmonisation go?
- What roles should the CESSDA SP's have here?
- Is there a central reference point for these activities?

The relatively small number of questions here indicates that the "data harmonisation activities" are abstract in nature and it is unclear to Service Providers what CESSDA's expectations are. This is related to the services CESSDA aims to offer. It's a task for 'Harmonisation' workgroup (one of the CESSDA Workgroups) to set a proposal, time frame, technical specifications, metadata requirements and guidance on that matter.

**9. contribute material and/or expertise to the cross-national question bank**
Questions from the Service Providers:

- Is this an existing CESSDA activity? Is there a working group, or will one created?
- What roles should or will the CESSDA SPs have here?

The Euro Question Bank project is one of CESSDA's Work Plan Task Projects and runs from 2015 to 2018. This Obligation is related to Obligation 1 about metadata and Obligation 8 about data harmonisation activities. The questions about this Obligation (and several other Obligations) indicate clearly that the Service Providers don't have enough information about ongoing work.

**10. provide mentor support for CESSDA ERIC Observers and their representative Service Providers to achieve full Membership**
Questions from the Service Providers:

- Would this support be in the form of events, active support, and guidance, or something else?
- How such activities would be organised and monitored?
- What would be the degree of central management?

Service Providers seem willing and able to provide mentor support but what is expected of them is unclear. It is also unclear how these activities should be reported. It should be decided, for example, whether providing mentor support should be carried out by individual "mature" SPs and/or in the form of training events and/or a permanent working group. Monitoring SPs progress in fulfilling the Obligations would help to direct mentor support in optimal way.

**11. provide member support for countries with immature and fragile national infrastructures to help them build up needed competence later to be able to fulfil tasks as Members**

Questions from the Service Providers:

- Should this read 'mentor support' like 10 above or does this refer specifically to full members providing support to others outside CESSDA?
- Would this support be in the form of events, active support, and guidance, or something else?
- How such activities would be organised and monitored?
- What would be the degree of central management?

The comments about Obligation 10 are valid here, too. It is worth noting that the SERSCIDA project (and later on SEEDS and SaW) is a good model for cooperation where teams from 'candidate' countries work together with the purposefully selected group of CESSDA members and their teams on consecutive tasks, that finally enable the operational data service prototype to be delivered in the 'candidate' countries.

Results and deliverables of those projects can be used for guidance and training. SaW Task 3.3. delivered a set of template documents about the generic data archive with the instructions, how to plan and adapt to specific circumstances. Also, SaW WP 3 results are, as a whole, meant to support the Strengthening and Widening of CESSDA.

Both Obligation 10 and 11 are similar in content. There has been a proposal submitted about a continuance of the widening activities (WP2018 - widening activities). Widening is also in the job description of the CESSDA Director. Both can include the mentoring suggestions that are best suited for a particular country that seeks support.

Obligation defined and measurement of the compliance can be set as a minimum activity that is expected from the SP, when asked for support from either country representative or the Director.

Training events and activities performed by CESSDA Training hub could deliver required content.

**12. facilitate access to national government and research funded relevant data, dependent on national legal systems**

Questions from the Service Providers:

- Is this via the CESSDA portal?
- Is there a clear persistent identifier need here?
- In addition to national legal systems there might be national guidance or best practices.
- Remote Access facilities are an essential point here.

- How can a SP demonstrate that it has facilitated this?
- This point should be more stimulated. How far is this within CESSDA? Should reminders be sent out to the SP's on this?
- How are the "Data without Boundaries" project's results reflected?

Many of above questions are related to other Obligations and will be solved once they are solved (for example, Obligation 1 about metadata and Obligation 3 about harvesting).

Service Providers need guidance on what is expected and how they can show that they are adhering to this Obligation. CESSDA could, for example, recommend that the SPs collaborate in national and international solutions to provide access to sensitive data.

Regarding national government data outcomes of DwB project, in particular suggestion of an European Service Centre for Official Statistical Microdata – ESCOS are relevant to consider, SaW task 3.4 future directions and recommendations from a report by the "OECD Expert group for international collaboration on microdata access" (http://www.oecd.org/std/microdata-access-final-report-OECD-2014.pdf).

Research funded academic data access provision depends on the national funders policy requirements. Promotion and training on RDM (Collaborative data management module for comparative social science researchers), and Data discovery training workgroups can support implementation.

Since there is no current workgroup on the topic, the CESSDA Director may take responsibility of defining the requirements.

**13. adhere to CESSDA ERIC's Data Access and Dissemination Policies**
Questions from the Service Providers:

- What is the policy in practice?

CESSDA's Data Access Policy was a Work Plan 2015 project and the policy was agreed by GA in June 2016.

Since there is no current workgroup on the topic, the CESSDA Director may take responsibility of defining the requirements.

**14. adhere to the provisions of the Organisation's policies as required**
This is rather obvious (in a way) and the SPs don't seem to need further elaboration.