A National Preservation Solution for Cultural Heritage

Juha Lehtonen, Heikki Helin, Kimmo Koivunen, Kuisma Lehtonen, Mikko Tiainen
CSC – IT Center for Science
P.O. Box 405 (Keilaranta 14)
FI-02101 Espoo, Finland
+358 9 457 2001
{juha.lehtonen, heikki.helin, kimmo.koivunen, kuisma.lehtonen, mikko.tiainen}@csc.fi

ABSTRACT
We present the status of digital preservation at the National Digital Library (NDL) of Finland. The NDL has created a nationally unified structure for contents and services ensuring the effective and high-quality management, dissemination, and preservation of digital cultural heritage.

General Terms
Institutional opportunities and challenges; Innovative practice.

Keywords
Digital preservation, open source software, hardware

1. INTRODUCTION
The National Digital Library of Finland (NDL) is an entity within the remit of the Ministry of Education and Culture within the Finnish Government. The NDL ensures the preservation of digital cultural content, providing access to and compatibility of content, designing a cost-effective digital preservation solution, promoting the cooperation between the national libraries, archives and museums (partner organizations), and building better services with open cooperation and expansion to include a large range, and amount, of content.

Almost all memory organizations under the Ministry of Education and Culture of Finland are obligated by legislation to preserve cultural heritage. A major share of content owned and administered by partner organizations consists of digitized documents and photographs, but the volume of born-digital content is expanding quickly. Given of the diversity of the partner organizations, the digital content to be preserved makes up a very heterogeneous landscape. Based on extensive surveys conducted among partner organizations, we roughly estimate that digital information stored to our digital preservation solution by 2020 will consists of more than 2400 million objects requiring more than 12 petabytes of storage space not including necessary replication[1].

The NDL's digital preservation solution was taken into production during 2014 with about a half of a petabyte capacity. Although current capacity is somewhat moderate, our architecture is built to accommodate the increased volume and diversification of content and organizations, as well as the possible development into a storage system for the preservation of research data. In the spring 2015, the NDL's digital preservation solution was awarded the ISO 27001 information security certification, and we are planning for future auditing with preservation related standards, such as DSA (Data Seal of Approval) and ISO 16363.

The key activity in our solution to tackle preservation challenges is actively maintain a standard portfolio, which defines the standards to be used in the NDL. The national standardization ensures the functionality of the composite system, which requires semantic commensurability of metadata by partner organizations. All NDL specifications are produced in a close cooperation with partner organizations[2].

The standard portfolio, however, does not give detailed instructions for implementation or application of standards, but those are produced separately. The NDL METS profile defines a unified structure for Submission Information Packages (SIPs) and Dissemination Information Packages (DIPs). With a common digital preservation service for diverse organizations, the unified structure of information packages enables efficient administration of the information on the long term and also enables semantically commensurable information content. Having a common and mutually agreed format for both SIPs and DIPs helps partner organizations to build their own systems in a sustainable way.

Further, the NDL has specified a closed set of file formats that are accepted to our digital preservation service, with requirements of mandatory technical metadata elements for each content type. Currently, our digital preservation service supports two kinds of file format categories: Recommended and acceptable for transfer. Recommended file formats are such that the NDL considers to be usable for a long time, whereas acceptable for transfer are formats in which a significant amount of content is currently stored within partner organizations.

2. DIGITAL PRESERVATION SOLUTION
The software layer of the preservation solution implements the technical side of the digital preservation services by following the OAIS reference model. The software architecture consists of front-end (services for the partner organizations and for the system administrator), back-end (functionality and coordination services for task execution), and services for the storage.

Our digital preservation solution uses a highly modular microservice structure, which means that the architecture is divided into small, highly independent components. Such a component may be a 3rd party open source or an in-house software, which takes care of a certain part of the implementation. Also, we employ the idempotence property for the microservices, which means that a task in a workflow can be run several times so that the repetition does not affect to the final result nor functionality of the preservation solution. In other words, we are able to repeat the interrupted microservices, and skip the succeeded ones without clean-ups. Modularity is also necessary for ensuring the continuity, since the existing component can be replaced with minor changes in the implementation. We employ open source software Luigi for managing the distributed workflow and MongoDB for the operational and metadata databases, as examples.

The partner organizations create SIPs according to commonly agreed national specifications. A SIP is technically a directory, where the NDL METS document and a digital signature file is located in the root level, and digital objects are either in the same level or in subdirectories. The partner organization transmits the SIPs via SFTP to a buffer of the digital preservation service. The workflow manager can then find the transferred data from the buffer and start processing it. The ingest workflow has several microservices for validating the data according to the NDL specifications. Each of these microservices generate a validation report, which are finally combined as a final ingest PREMIS report.

Each AIP is packed in a Bagit format, which contains the accepted SIP and the final ingest PREMIS report. This construction is then wrapped in a compressed tar format. AIPs are finally moved to a storage buffer, which stores them to one disk media type and two different tape media types. To avoid possible technology dependency issues and/or technology lock-in, the three copies are stored with three different storage technologies produced by different manufacturers. In the first phase system, the storage media formats are: 1) Nearline SAS 4TB disks with RAID60 technology; 2) magnetic tape, Oracle T10000D drive with T10000 T2 media type; and 3) magnetic tape, IBM TS1140 drive with 3592 JC media type. We also have a dark archive service as an ultimate backup. This results that three active copies and two dark archive copies of all AIPs are stored.

Multiple servers are used for controlling the front-end, databases, disk storage, and tape libraries. The actual disk storage capacity is currently 728TB, which is distributed between five different big data oriented servers providing also processor capacity for operations in software layer, such as for ingest, dissemination, and preservation actions. Scaling out to more servers extends both disk and processor capacity. The tape libraries, in our case Oracle StorageTek SL8500 and Spectra Logic T-Finity, scale up to thousands of tapes, which makes a capacity of several petabytes possible. The tape library interfaces are open source components, and the file system employed for the tapes is a common open source standard LTFS, and therefore, the stored data can be read from the tapes even if the manufacturer discontinues supporting their own implementation. The system is connected with a redundant 10 Gbps connection to a fiber backbone network of 100 Gbps speed.

Development in hardware advances rapidly. We estimate that life cycle of the disk storage, tape drives and magnetic media types are five years, and life cycle of the tape libraries are ten years. Therefore, the hardware architecture is planned in a cost efficient way, so that we can afford to accept the fact that disks and tapes eventually get outdated, and it is business as usual to renew those. The architecture is built so that media failures do not have any effect on the preserved data nor the services, and replacing new disks is a low cost operation. Periodic bit preservation actions are also automatically performed for the data, and replacing the corrupted copies is a fully automated process.

The digital preservation service provides management tools of preserved data for the partner organization and for the system administrator. These are, for example, tools for following the ingest process or preservation actions, tools for preservation planning, and tools for updating or removing the data. The partner organizations can manage and follow only their own data. In the near future, our digital preservation service will also perform file format migrations and other logical preservation tasks to keep the data accessible and usable. This will be done in a close collaboration with the partner organizations by conforming to their preservation plans.

Our solution is dynamically scalable with practically any amount of data. The key in the scale-out technology is to distribute the storage and processor capacity between servers. Distributed file system technologies are used for this purpose, and we have chosen an open source file system GlusterFS, which takes care of the actual disk storage and a separate processing buffer for actions, such as ingest, storing, and dissemination. The connections from the partner organizations to the system are formed to a randomly selected front-end server with using a dynamic DNS bound to keepalived offered virtual IP addresses for a front-end servers available. This distributes the traffic between the digital preservation service and the partner organizations evenly between the servers.

Secure HTTPS protocol is used for all data management and access. An authenticated user can search granted data, create and download DIPs, get reports about preservation events, and get statistical information. Here, a REST interface is designed especially for automated access, and a web application using the REST interface is developed for the manual use. In the future, various additional management and access services will be developed.

Our system integrates about 40 existing (3rd party) open source components and about a dozen in-house components together. The integration work between software components, databases and services are produced in-house using the Python programming language. Selecting the 3rd party components includes an evaluation process before the actual deployment. At first, those software candidates are selected, which fulfill the needed functional requirements. The evaluation is usually done with a small but comprehensive test task, which will be implemented with the different candidates separately. These accepted candidates' maturity is then evaluated with using a method based on the QSOS (Qualification and Selection of Open-source Software) version 2 evaluation method.

We presented our national digital preservation solution concentrating on its software implementation and the hardware architecture. At the moment, the preservation services are utilized by national memory organizations preserving cultural heritage, but the services are under development for research data.

[1] H. Helin, K. Koivunen, J. Lehtonen, and K. Lehtonen. Towards Preserving Cultural Heritage of Finland. In Proceedings of the Cultural Heritage on line – Trusted Digital Repositories & Trusted Professionals, Florence, Italy, December 10–14, 2012.

[2] http://www.kdk.fi/en