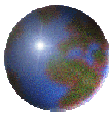


Trusted Digital Repositories: OAIS and Certification

Robin Dale
RLG
Robin.Dale@notes.rlg.org

Could be any or all of these.

We know that to preserve our nation's records and cultural heritage, we will need to have a networked (at least loosely) group of repositories capable of being trusted to preserve that content.

And being networked implies the ability to work together and to trust each other – to exchange files or perhaps instead rely on certain institutions to preserve some content while other institutions preserve others.

With those minimal requirements, we begin to see that we have some firm needs emerging.

All of these things were addressed by the RLG/OCLC Working Group on Digital Archive Attributes. The final report was recently issued. [SLIDE]

What does the report do?

1.) Provides a definition of a *trusted* digital repository

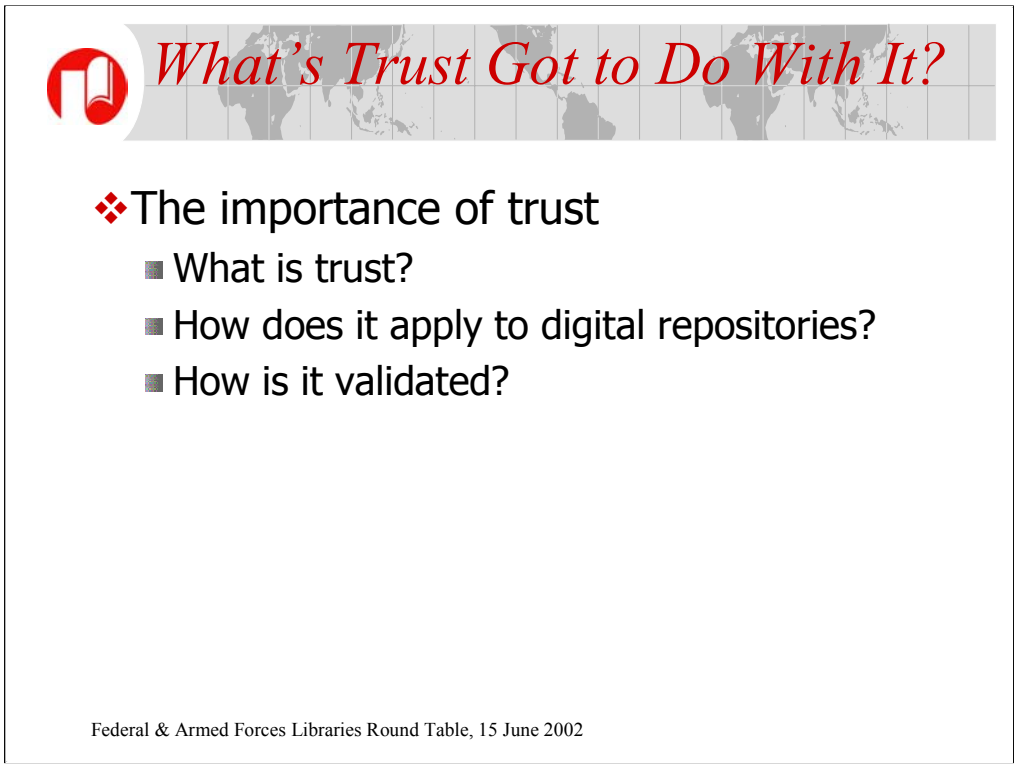
2.) Identifies the primary attributes of a *trusted* digital repository

3.) Identifies the responsibilities of an OAIS-compliant repository

4.) Articulates a framework for the development of a certification program

Three main issues I'll discuss from the report and from our ongoing work.

Let's start with Trust…



There is a need for a mechanism to gauge and hold trust of and in a digital repository

.

Well we know that trust must exist on a variety of levels. Minimally, three levels of trust apply to the establishment of trusted digital repositories:

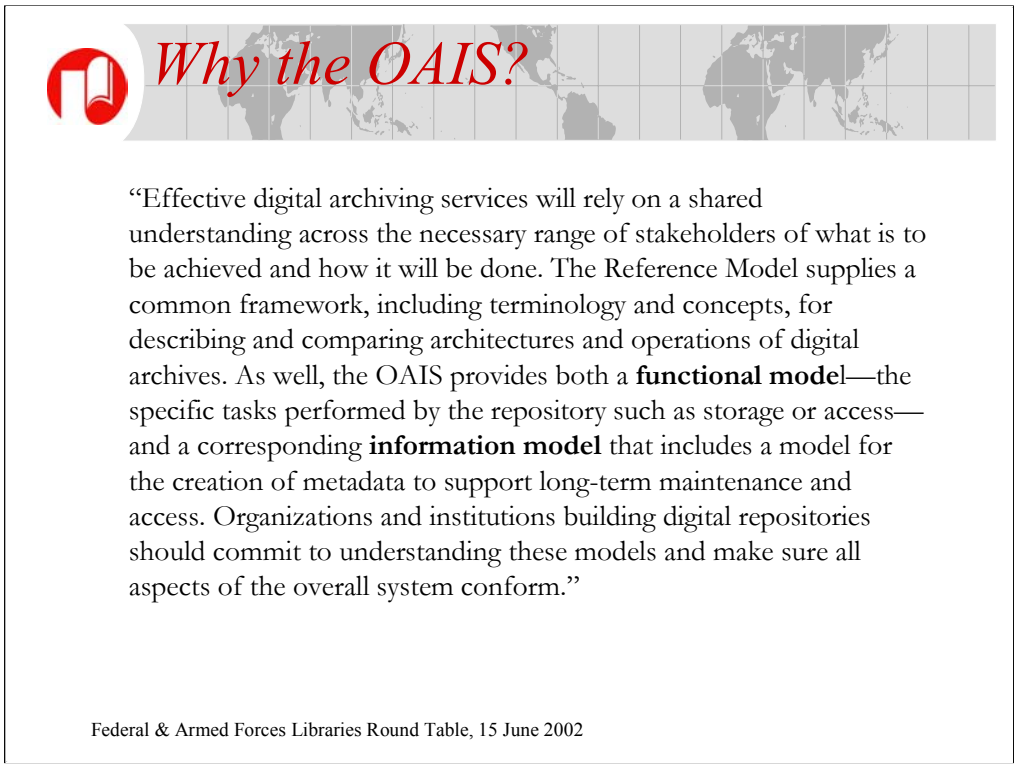
1. How cultural institutions earn the trust of their designated communities.
2. How cultural institutions trust third-party providers.
3. How users trust the documents provided to them by a repository

But how can trust be translated into a measurable mechanism?

Validation is more difficult. How do we "validate" the trust we have in other things? Why are libraries, archives and museums now entrusted with our nation's cultural heritage? They are trusted to store these valuable materials. They are trusted to provide access to them in order to document and reveal history as well as to foster the growth of knowledge. They are trusted to preserve these items to the best of their ability for future generations. Cultural institutions have excelled in preserving large amounts of cultural heritage in the form of physical objects. In many cases, these physical objects or documented, reliable surrogates are available to patrons as "proof" of the institution's capability to collect and preserve for the long term. But since digital information is less tangible and much more mutable than other materials, trust and reliability may be more difficult to prove.

I mentioned that the report lists attributes and responsibilities of trusted digital archives. I'm showing you the list of the seven attributes identified. As you can see, Compliance with the OAIS reference model is at the top of the list.

But why the OAIS?



This paragraph is a direct quote from the report:

[READ]

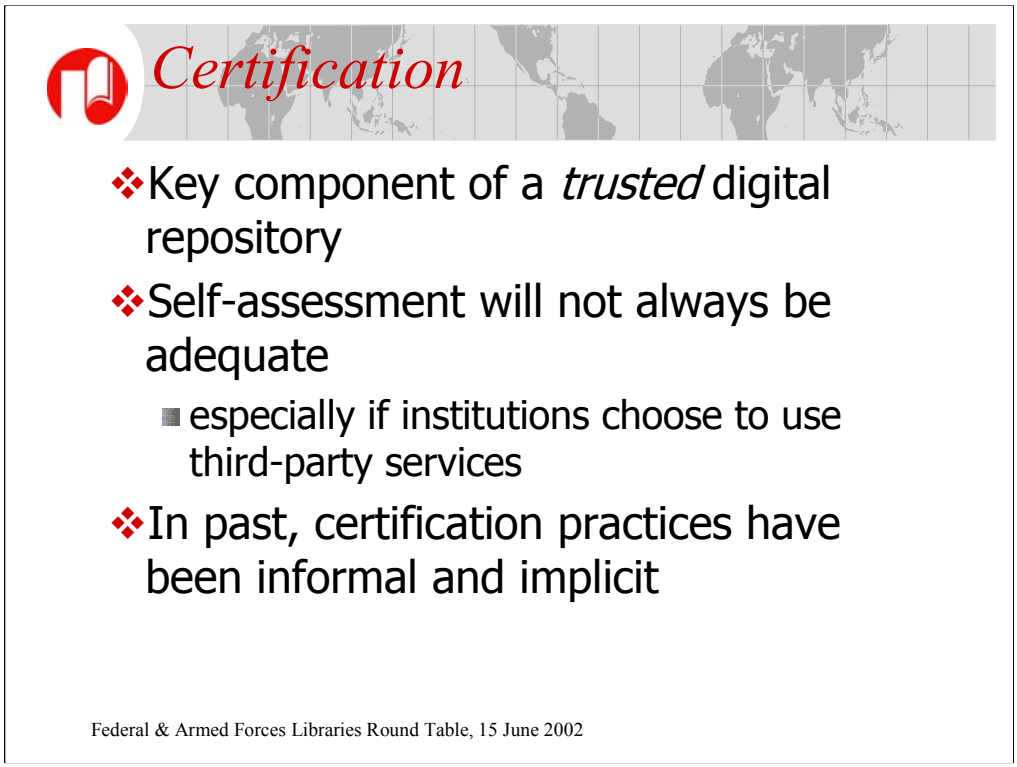
So the paper doesn't describe what an archive must look like or even how it must behave. We will not have a networked group of IDENTICAL repositories out there, but if we can make sure that digital repositories are compliant with the OAIS, we already know something about them. It is a basis for the trust that must be developed.

Remember that one important level of trust is that cultural institutions must be able to trust third-party services. If third party services are OAIS compliant – or perhaps fulfill one aspect of an overall OAIS-compliant system – we can begin with a shared understanding and move more easily toward trusted relationships.

OAIS & Certification

"The OAIS reference model does not address the issue of certification of archives directly. Nevertheless there is considerable interest, particularly when one archive needs to rely on another for a range of services, in being able to 'trust' the other archive. One way to approach this in general is to identify approaches by which an archive may establish some level of certification, whether by self assessment or by an auditor."

Federal & Armed Forces Libraries Round Table, 15 June 2002

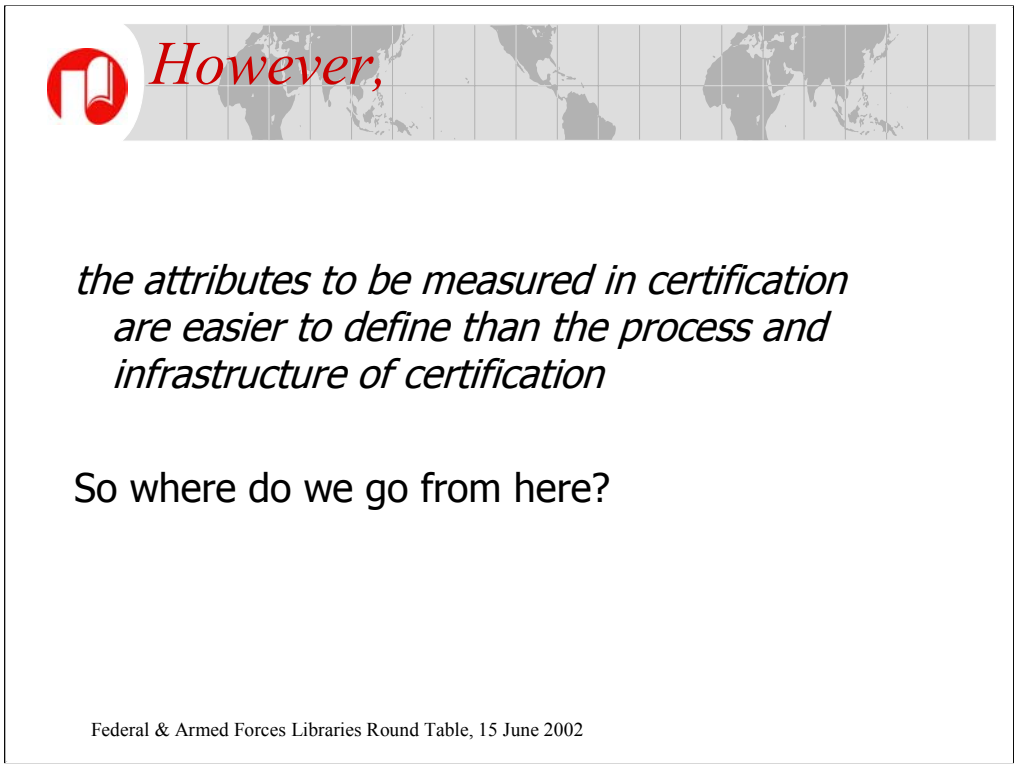


Why certification?

Development of trust, as I mentioned earlier, usually takes place over a long period of time. With digital preservation, we don't have the time to waste. We need immediate action. So what can we do? How can we approach digital preservation in the short-term so that we can build it for the long-term?

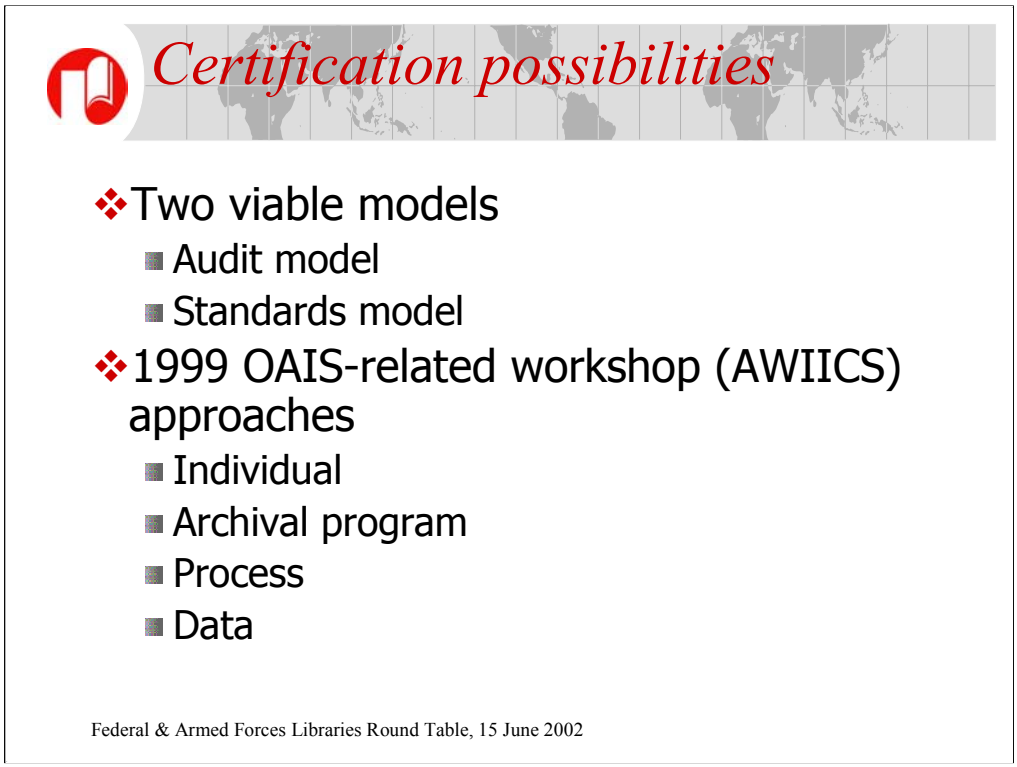
Certification. It becomes a key component of contemporary digital repositories. In the breach, we use certification as our mechanism and gauge. This allows repositories to get up and going, get business, build and prove good practice. And over time, they'll earn our TRUST.

In the past, certification practices have leaned towards the informal and implicit. With digital repositories, there is a desire – perhaps a need - to see certification be formalized and made explicit.



Interested communities and experts can & should develop a program for certifying trusted digital repositories

Checklist concept and certifiable elements provide a base for developing a certification framework



Draft report outlines existing types and models of certification,

•Audit model The audit model is applicable to depositories holding government records, especially electronic records. In the US, such depositories must meet guidelines created by legislation or by agencies such as the Department of Defense.

•Standards model: The standards model operates in various places in the library and archives community. Two examples are guidelines for producing preservation-quality microfilm and ISO interlibrary lending. Institutions involved in these activities adhere to standards established by appropriate agencies. Peer institutions "certify" the product or service by their acceptance and/or use of it.

While both models work well, neither can completely address the range of activities, functions, and responsibilities associated with digital repositories.

Four certification models refine the standards and audit models: four general approaches to certification: individual, archival program, process, and data.

The participants in the AWIICS workshop agreed that elements of each of these four processes could form a certification program that provides layers of trust. A layered

Complementing the attributes framework outlined in an earlier section of the report, the next step is to identify a certification framework.

The report outlines an entire certification framework, but recognizes that several key components are identified and discussed already. The entire framework is shown here. I think you can see that the first few points have been addressed – We have determined the need for certification, and the need for an official certifying body, and finally, identifies a framework for attributes to be measured.

Next steps

- Certification effort surging forward
  - Core group from RLG, NARA with interest from Cornell, Harvard, OCLC and others
- Tools for OAIS implementers
  - Discussion list for practitioners
    - oais-implementers@lists2.rlg.org
  - Web site of organizations using OAIS
    - www.rlg.org/longterm/oais.html