References to the prerequisites for TDO interpretation would introduce a security loophole if they were used without further ado. Were such a referent to be improperly altered before its use, the result could mislead the eventual TDO consumer. Conceivably, some clever criminal could exploit this weakness to perpetrate widespread fraud. Doing so would be particularly easy with unprotected UVC programs. However, this loophole is readily addressed. Wherever the TDO architecture described above calls for an included TDO identifier, it should be accompanied by the associated MAC and the public portion of the asymmetric key pair used to sign it. With this, a suspicious consumer could immediately check whether the referenced TDO is what the producer referred to. Such checking could, and perhaps should, be built into TDO retrieval procedures.

11.2 Infrastructure for Trustworthy Digital Objects

A certification—an unforgeable signed sealing with a message authentication code, can make a bit-string reliable for some applications. Authenticity evidence must be based on the security and credibility of records of producers' identities and their cryptographic private keys. These, in turn, must be based on facts that people—the public at large—trust. The intended clients of a certifying institution might include the entire citizenry of a large geography. We can engender their trust by grounding claims on relatively simple public assertions by some institution that has little to gain and much to lose by misrepresentation of the information it publishes—an institution, such as a national library, that is widely trusted to handle documents like the one in question correctly and faithfully. We call such an institution a *trustworthy institution* (TI).

A TI assertion might be represented by a WWW and newspaper publication of its own public key, which it announces will be used in signing certificates and message authentication codes, and an offer to issue identifier certificates to certain organization classes. For instance, each of a dozen or more national libraries or archives might advertise something like, "La Bibliothèque nationale de France (BNF) offers certification of the public key of any [some class of institution] that provides [certain information about itself] by a visit of its accredited representative to BNF premises. The BNF public key from [beginning date] to [end date] is [key value]." From a few such starting points, we could create a network of interdependent facts that will allow a TDO recipient to evaluate claims of veracity and authority made in and about the TDO.

Part of what a TI must do to qualify itself is to publish its certification criteria and to persuade its intended clients that the institution depends in essential ways on its reputation for integrity and competence.

Furthermore, it should submit to occasional independent audits of the adequacy of its external commitments and its compliance in its internal workings with these commitments. This would be a much simpler audit than that called for by RLG (§8.4). It would check adherence to the quality specifications for acceptable input and production of new TDOs, as well as the management controls on the use and protection of the institution's private keys. Many programmers have the knowledge needed to perform such an audit.

The certification criteria would typically include specific requirements for each document's metadata, and also submission by an agent the TI knows and trusts for such submissions. To help manage a large traffic of certification requests, compliance testing can be at least partially automated (in the Digital Object Import module of Fig. 26). Each proper TDO would include or refer not only to a MAC signed by its producer, but also to descriptions and identifier certificates of every individual producer in its history (or cryptographically secured references to such certificates). Each TI agent who certifies a document acts as producer who should diligently judge the authenticity of information that he will certify. Flawed certifications will jeopardize the reputation for integrity and quality that creates and maintains the trusted status of his employer.

A TI can enlarge the community that might trust the works that it certifies by persuading other TIs to certify its public keys using public key identifier certificates conforming to the X.509 standard.[402] Each such TI would participate in creating a web of trust (§8.1.4) by publishing the public key certificates it has signed to endorse the public-key-to-identity mapping of its sister TIs. Such mutual endorsement can be made safe against "man in the middle"[403] attacks by institutional agents exchanging public keys in face-to-face meetings. The benefit to each participating TI would be a reciprocal endorsement.

11.2.1 DO Certification by a Trustworthy Institution (TI)

After a TI receives information from its producer, it must test this input and its knowledge of the producer to determine whether these satisfy its own published criteria for document certification. If they do, it should create a new DO by copying, editing, and augmenting the input metadata with a new metadata block that conforms to standards and to its own published specifications. When this editing is complete, it should copy the resulting DO into a signing computer (SC in Fig. 26) that it can detach

402 Gerck 1998, *The Unabridged X.509 Certificate.*

403 Schneier 2000, *Secrets and Lies: Digital Security in a Networked World,* p. 48.

from the Internet in order to protect the sensitive signing step and its private key from Trojan Horse attacks.

Whenever it contains a sufficient input batch, its operator must detach the SC from all networks and then load it with the TI's private (secret) key. The operator will then start a utility program that (1) tests that each input meets all TI-required quality criteria, (2) fills in missing PB portions into each input, including metadata for the pending MAC, and (3) computes and adds the MAC, thereby finishing the TDO construction. Finally, the operator must remove the private key from the SC before he reattaches that computer to networks to send the newly certified TDOs to wherever they are wanted.

To assure users about the age of the TDOs it has sealed, and to protect its private key further, the TI could choose a new public/private key pair periodically—annually for instance—and destroy all copies of the expired private key. It should further publish the history of its public key values.[404] This mimics an eighteenth and nineteenth century Japanese practice, in which the censors of ukiyo-e ("pictures of a floating world") changed their seals approximately annually, doing so over a period of 200 years, and published these keys (Fig. 36) so that each became evidence of the print date of the pictures on which it recurred.[405]

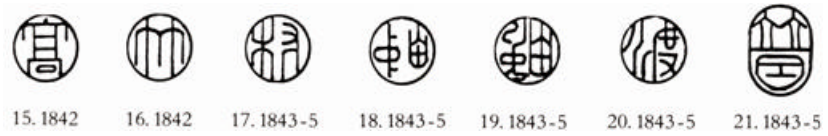

Fig. 36: Japanese censor seals: ancient practice to mimic in digital form

The SC should be exclusively devoted to creating institutional MACs that convert DOs into TDOs as a security measure for protecting the private key of the TI. Whenever it is attached to any network, the SC must be guarded against containing any TI private key. It might more securely protect the private key never to attach this security computer to the network. Instead, one can transfer objects requiring certification onto a Write-Once CD, using this as input for sealing, and transfer the resulting TDOs back to a networked machine with a fresh Write-Once CD. By checking that the input CD contains no stowaway files, this procedure would make virus invasions unlikely. (The input files need never be executed on the SC, so that the risk of virus entry opportunity is avoided.)

404 Maniatis 2002, *Enabling the Archival Storage of Signed Documents*, suggests a different solution. See also Wallace 2000, *Trusted Archive Protocol*, http://middleware.internet2.edu/pki04/proceedings/trusted_archiving.pdf.

405 Illing 1980, *The Art of Japanese Prints* , p. 170.

A TI would make misappropriation of TI private keys difficult if it followed the above procedures and also conformed to administrative security controls. How carefully this process and related procedures need to be managed will depend on the kinds of information that the private key will be used to certify, for example, keys for military applications will require more care than keys for scholarly publications.

11.2.2 Consumers' Tests of Authenticity and Provenance

Accumulating certificate signing events described will elaborate Fig. 23 to create a Fig. 37 web-of-trust-based certificate forest.

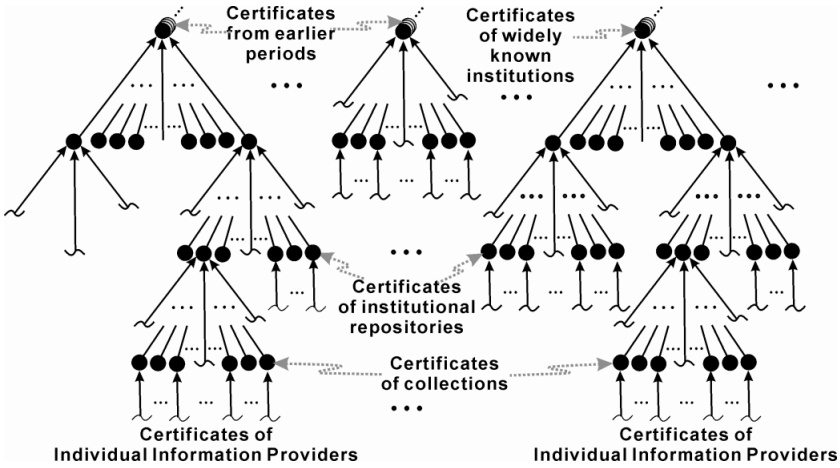

Fig. 37: A certificate forest

A cautious consumer will not judge a received TDO to be authentic unless he believes certain things:

- That the enclosed MAC demonstrates that the TDO has not been altered after it was certified;
- That the enclosed identifications of the most recent MAC signatory and date are authentic;
- That the producer of each stage in the TDO's history had the authority to make her/his changes;
- That the final signatory's procedure for generating TDOs is sound and includes judging the authenticity of information it includes in any TDO it creates; and
- That the TI (trustworthy institution) signing procedure has been correctly executed.

As evidence, the consumer will have the published public keys of the world's TIs, endorsed by other TIs' cross-certifications, and the certified public keys and known identities and roles of TDO producer chains, which are carried in TDOs. If each TDO embeds all its prior versions, the consumer will quickly be able to identify the specific changes made by each producer. The consumer might additionally be able to judge the TDO payload (Fig. 32) as corroborative evidence and might also use the context provided by other documents that he knows professionally.

Locating such certificates, certificates for signatories of each interesting identifier certificate, and producer descriptions whose content the consumer chooses to inspect are graph traversals.[406] That each document referred to is the correct object is validated by comparing its MACs to the MAC value stored within the link at the time it was constructed.

The correct rendering (for human consumption) of a collection member is likely to depend on the correctness of other information objects, some of which might not be in the collection. Even if an object is protected so that its bit-string source is known to be authentic, changes in the objects on which its rendering depends might mislead its user. For sensitive objects, this poses a security risk that should be mitigated by time stamped MACs within the rendering tools used and checked.

A software tool is needed to help the consumer inspect a TDO and extract portions of interest. He might have received the TDO in e-mail from its producer or from a third party. With the appropriate tool he will be able, without further ado, to extract and exploit blobs that interest him. He will also be able to use PB contents together with published key values and published TI acceptance policies to assess to what extent he will trust TDO payload components. This task can be automated if the endorsing TI has expressed its quality criteria as production rules of the kind used in artificial intelligence applications.

This tool might be a Web browser application similar to today's interactive research library interfaces. The challenge is to make it intuitively convenient for untutored users, who should not need even help text to formulate queries or traverse reference and certificate networks. Such a search service crawler would exploit other information in each PB immediately, including its semantic relationship information.

Search services should provide for returning URL sets of at least three different kinds: (1) URLs satisfying the query; (2) all URLs of (1) augmented by URLs whose DRIs coincide with those found in the response (1); or (3) the response (2) pruned to remove URLs for duplicate TDOs. The graphs of related documents would be easily constructed.

406 Caronni 2000, *Walking the Web of Trust* discusses optimal traversal algorithms.

Graphical interfaces might be convenient to browse and traverse relationship networks.[407]

11.3 Other Ways to Make Documents Trustworthy

§11.2.2 suggests basing consumer's authenticity testing on the validity of a cryptographic key. This key is recursively testable for validity according to an acyclic graph of public keys that are rooted in the published keys of a few widely known institutions (Fig. 37). Each step of the certification chain can be tested to check that it has not been falsified. This method works because its execution is easily controlled administratively, because it is easy and inexpensive to apply, and because responsibilities are partitioned so that it would be against the interests of certifying institutions to permit fraud.

Waugh suggests another method of showing that a particular public key belonged to a particular signer at the time a preserved object was signed.[408] A well known publisher might use the same certification key-pair for many works. The user interested in the authenticity of a work issued could check whether its public key value is identical to that of a body of works from the publisher. This is likely to be acceptable to a user who is satisfied with knowing that the work is truly from the alleged source.

As an example of why this makes sense, consider the outré case of someone who wants evidence that a certain play is by William Shakespeare rather than by Christopher Marlowe. Unless this reader is interested in the narrow historical question of whether the true author of all Shakespeare's plays was in fact Marlowe, nobody really cares about the connection of the plays to a particular collection of buried bones. What might be interesting is whether the author of *Cymbeline* is the same as that of *Hamlet*.[409]

Yet another method of time certification is based on the administrative independence of repositories belonging to and managed by unrelated institutions. If the same document has been independently stored in several individually credible repositories, its eventual consumer can test whether the supposedly independent instances are sufficiently similar. For this to be proof against fraud, there must be accessible, unforgeable evidence that the document's producer himself delivered each instance to a credible inde-

---

407 *Aduna Autofocus* exemplifies such graphical browsers; http://aduna.biz/products/autofocus/.

408 Waugh 2002, *On the use of digital signatures in the preservation of electronic objects*.

409 For amusement, see the Christopher Marlowe anagrams at Shakespeare's grave, available at http://www.geocities.com/chr_marlowe/shakespeare_epitaphs.html.

pendent repository, rather than that a single deposited instance was copied among repositories.

This might be made verifiable by the firm binding of each repository's credible assertion that it received its instance from the producer rather than from some third party—a provenance certificate for its holding. For cautious consumers, the solution must be proof against independent misbehavior by anyone, including any repository employee. Any reader who cares to do so can surely work out the details whereby a repository can test, prove, and certify that the provider of a document copy is also its producer.

11.4 Summary

When information is cryptographically packaged together with its own provenance assertion, and this evidence shows itself to be intact, a consumer can be confident that the information is authentic. We call a data object packaged this way a Trustworthy Digital Object (TDO).

One can transfer the loci of trust from numerous objects that are individually relatively large to a few small objects—from document copies to a few cryptographic keys whose secret portions are the private keys of a few widely trusted institutions. These private keys can be protected easily and inexpensively against improper disclosure. The TDO method binds three generic sources of trust—information with which a consumer can decide whether to trust the provenance and integrity of a TDO, i.e., the context of cited documents, especially linked TDOs, whose contents can be judged for consistency with the content at issue; access to previous TDO versions, either by including them in the TDO payload (Fig. 34) or by their availability by Internet searches based on shared resource identifiers; and links to descriptors of each TDO's producers and, through them, to a network of identity certificates rooted in the public keys of respected institutions.

Most documents will rely on other documents for their reliable interpretation. Such dependencies will be highly recursive, but can be grounded in a small number of documents that articulate data processing standards, such as ISO Unicode, and ontologies for the topics at hand. This leads to heavy use of links and to our needing graphic programs for conveniently navigating dependency graphs to show the values represented within each node.

Object encapsulation and sealing are not new ideas. TDO properties that make it possible to test authenticity include the following:

- Each TDO package includes all metadata needed as evidence of its content blobs' provenances; these metadata are *OAIS*-compliant.