

Miscellaneous

M1. UPDATEABLE PUBLIC KEY

The public key of a Handle is a Handle. Public keys can be updated through Handle and retrieved transparently.

- Public key for an encryption is assigned an identifier.
- Identifier resolves to the public key.
- Encryption based authentication services can operate on identifier for key, rather than key itself.
- Key is updated, and resolution on identifier system is updated.
- End user needs make no change; user only uses the stable identifier to the key, and redirection of identifier to new key is hidden from user.
- This is yet another example of a service operating on an identifier that is not an HTTP resolution service (though it is arguably still a resolution).

M2. LINK ROT CHECKER

A link-rot checker is a core service for identifier management systems, which ensures the persistence of identifiers. Persistence in identifiers is a matter of policy more than infrastructure; it makes much more sense for managed data than unmanaged, and it is easier to manage one's "Own Stuff" than "Their Stuff". To police persistence, a persistent identifier system can require registration of identifier accountability. That way, a path of escalation to is available if the identifier manager fails to maintain the identifier resolution persistently.

Given the accountability data, a periodic process can be initiated of validating the identifier: if the identifier is found to be invalid, the accountability data allows redress to be sought. At the most basic level, we assume identifier resolution to a URL, and verify that the URL is live. (Validating that the URL locates the same object is more complex, and may require digital watermarking.) More generally, we can go through all metadata about the resource held in the identifier system (both core and peripheral, and both resource metadata, including location, and descriptive metadata). For any metadata field whose value can be established through an automated process, the value is verified.

- An identifier is registered.
- An identifier is associated with metadata, including association data, and a manager responsible for the association.

- Periodically, an automated process verifies that the metadata values it holds for the identifier are still valid.
- If the association data has been realised as a locator, the process verifies that the locator remains a valid locator, which retrieves a digital object (where applicable).
- The process may also verify, given the right metadata on the retrieved object, that the object matches the discriminant metadata attributes recorded for it (i.e. that the identifier points to the same object it did before, as far as the metadata the system knows about is concerned.)
- If the process yields a mismatch or a failure, the identifier manager is notified to take remedial action.
- If no response is forthcoming in a reasonable period, the notification is escalated as appropriate.

Note



The identifier manager should be specified as a role rather than a person, so that it persists past changes of staffing, and so that an escalation pathway within the home institution of the object can be pursued. If an object is not housed within an institution large enough to allow for an escalation path, it cannot be regarded as well-managed, and its persistence cannot be guaranteed.

M3. IDENTIFIER FOR SERVICE

A service can be treated like any other digital object: it has associated metadata, it may change location, and it may have more than one deployed instance, subject to appropriate copy selection. The metadata for a service can include access profile, input and output specifications (e.g. WSDL), and a description of functionality. Mission-critical services in particular may need to be insulated from location change. By assigning a persistent identifier to the service, resolving to one or more locators, consumers are insulated from relocation of the service. If the service has metadata of a form consistent with that of first order digital objects, consumers can combine the two metadata records, e.g. to formulate an aggregate access profile.

- A service is assigned a persistent identifier.
- The identifier resolves to the service locator.
- An appropriate conduit is used to combine identifiers for the service and the service parameters into a service request at the service locator.
- The identifier persists in functionality though the service locator changes.

- The service identifier is keyed to metadata records, including access profile and description.
- Users can consult this metadata, and use it in combination with other metadata discovered through the identifier system.

© Copyright 2007	Legal 	Privacy		Powered by 
------------------	--	-------------------------	--	---

The PILIN project is funded by the Australian Commonwealth Department of Education, Science and Training, ([DEST](#)) under the Systemic Infrastructure Initiative ([SII](#)) as part of the Commonwealth Government's Backing Australia's Ability – An Innovation Action Plan for the Future ([BAA](#)) under the ARROW Project.