Specifications

In order to support these values and services, the DPN architecture is putting in place the following processes:

1. DPN will make multiple copies of content from a First Node to Replicating Nodes.
2. DPN will determine the number and location of copies based on policy.
3. DPN will audit the bit integrity (fixity) of replicated content upon all data movements to ensure faithful copies have been made.
4. DPN will audit the bit integrity (fixity) of content in Nodes on a periodic basis, to ensure faithful copies are maintained.
    a. A regular report of fixity checking will be made and retained for management purposes.
    b. DPN Depositors, First Nodes, Auditors, and DPN management will be able to access fixity check information on demand and through regularized reporting.
5. DPN will repair or replace any replicated content at any node when corruption is detected.
6. DPN will assure the security of replicated content during transmission so that no content is lost, corrupted, or exposed.
7. DPN Nodes will ensure the security of content at rest in replicating nodes so that no content is lost, corrupted, or exposed.
8. First Nodes may optionally encrypt content before it is replicated in the Network; for these cases, DPN shall maintain a key management system that safeguards access to the key(s) except by authorized parties (e.g., the First Node and/or Depositors), but ensures access to the keys upon successioning.
9. DPN will maintain an auditable record of actions taken on content during transmission, storage, maintenance, and restoration of content sufficient to demonstrate the provenance and authenticity of replicated content.
10. DPN will maintain a registry of replicated content to allow management of the network. **[1]**
    a. The registry will be designed and operated in a distributed fashion, and will be synchronized across all DPN Nodes.
    b. The registry will track the identity, source, location, and fixity of content in DPN.
    c. The registry will be designed and operated to assure the security and integrity of its information.
11. Replicating Nodes will operate at a level necessary to support the business and operational needs of DPN.**[2]**
12. DPN succession will align with Trustworthy Repositories Audit & Certification (TDR), specifically regarding succession planning, governance & organizational viability in section A1.2.
13. DPN Nodes will be designed, operated, maintained, and enhanced in a coordinated fashion to ensure diversity and manage the risk of loss due to correlated faults.
14. DPN will be able to scale up or down, including the abilities to:
    a. replicate new content at scale (in a reasonable timeframe)
    b. restore content at scale (in a reasonable timeframe)
    c. add new DPN Nodes
    d. tolerate the removal of DPN Nodes from the network
    e. “rebalance” the distribution of content among DPN Nodes
15. DPN will only delete content in accordance with defined policy.
    a. DPN will support confirmed and timely deletion of content as required by law and operational agreements of the First Node
16. DPN will be able to support the introduction or exit / cessation of DPN Nodes by redistributing content among new/continuing nodes to ensure sufficient copies are kept according to policy.
17. First Nodes should encapsulate or reference Representation Information (RepInfo) and Preservation Descriptive Information (PDI) for content sufficient to enable brightening by other DPN nodes or independent third parties in the event of cessation of operation by the Customer/First Node. **[3]**
18. First Nodes should encapsulate (or reference) rights / licensing information for replicated content sufficient to enable brightening by other DPN nodes or independent third parties in keeping with succession rights obtained and granted by the First Node. (see discussion in Endnote 3)
19. All content in DPN will be identified and packaged in a consistent way to facilitate identification, replication, restoration, and fixity checks.
20. DPN shall operate a messaging system with a common communication protocol to orchestrate actions among nodes.

[1] Network Management activities will comprise activities such as capturing data necessary for reporting, billing, internal logistics, load balancing, etc.

[2] Business / Operational needs of the Network could comprise activities such as demonstrated operations consistent with practices defined by the TDR reference model; demonstrated compliance with security standards such as PCI-DSS; participation in disaster recovery and “brightening” audits, to demonstrate the survivability of information in the Network.

[3] DPN will provide a large-scale network of dark archives that enable the opportunity to brighten content in the future, but does not mandate how this is done. Depositors, First Nodes and their designated communities will collaborate to ensure that the information contents of DPN deposits are accessible for reuse in the future, using the appropriate (and evolving) community standards for any given set of content.