Tufts University - Streamlined and secure way of distinguishing open from closed data

Usecase 2 - A streamlined and secure way of distinguishing open from closed data

Title (goal)	A streamlined and secure way of distinguishing open from closed data
Primary Actor	curator
Scope	
Level	
Story	the curator manages three collections: a completely open one, a mixed access collection (e.g. password-access to copyrighted materials), and a completely dark one (e.g. personally identifiable information). The cost to the institution of anything dark accidentally being made public is **high**. However, materials do sometimes intentionally move back and forth (bidirectionally) between open, mixed, and dark. The curator needs this process streamlined. Explanation: right now there are really two ways of distinguishing between a dark and an open Fedora collection. The wholly secure way to have entirely segregated Fedora instances on entirely different systems; This solution has minimal convenience. The wholly convenient way is to trust to XACML, FESL, or something higher level such as Hydra access controls; this solution relies on the shifting landscape of Fedora access controls for something with a high risk cost. Is there a middle ground between the two models?