Disable use of IdP internal encryption key

During installation, a special internal encryption key, referred to as a Cookie Encryption Key or "data sealer" key in various places, is generated. Various features that are enabled by default to support stateless clustering of the IdP depend on this key, along with some less-used features.

If you want to completely disable the use of this key and avoid having one at all, you will need to make a few changes to the configuration (V3.4.0 or later):

1. Comment out all the properties in *idp.properties* that begin with **idp.sealer,** particularly **idp.sealer.storeResource**.
2. Uncomment and override the **idp.session.StorageService** and **idp.consent.StorageService** properties in *idp.properties* to reference an appropriate storage service of your choosing,
3. Uncomment and modify the property named **idp.transientId.generator** in *saml-nameid.properties,* and set it to **shibboleth.StoredTransientIdGenerator**.
4. Edit the list bean named **shibboleth.ClientStorageServices** in *session-manager.xml* and comment out the two bean references (but **not** the list itself) inside it.
5. Switch the pre-configured CAS ticket service in *cas-protocol.xml* from the "encodingTicketService" to the "simpleTicketService" (these are bean aliases with documentation around them).
6. If you have enabled the **shibboleth.authn.Password.RetainAsPrivateCredential** bean in **authn/password-authn-config.xml,** you must turn it back off.

The IdP should then restart and function normally.