



PATTERNS

CRYPTO CHECKLIST

CRYPTO CHECKLIST

Y	Data treatment
Y	Use existing
Y	•••

Data treatment plan created and consequences accepted by management
Trust anchors identified and named
Sensitive operations (crypt,sign,) require client authentication (applies to services too!)
Existing (e.g. RFC 4880) protocols & formats used wherever possible
Nonces used only once. Random salt used where possible
Cryptographic concept written down & challenged in review
(Master-)Key offsite backup established
Key refresh after a few GiB of encrypted data implemented and tested
Algorithm rollover implemented and tested
Entropy source with enough entropy used
Test cases include restore of old data (key/algorithm rollover)