

Consensus - XML Encryption

Deployers **MUST** encrypt assertions and **MUST** use AES GCM as the encryption algorithm.

SPs **MAY** use a single RSA key for both decryption and signing in the event that they have a signing key.

Deployers of IdPs **MUST** use separate encryption and signing keys (if we end up requiring IdPs to decrypt, otherwise moot).