TrustManagement

TrustManagement is a convenient term for how Shibboleth uses cryptography to secure SAML messages and assertions. Trust is an overloaded word, but here we mean simply the binary choice that the software has to make: does this bag of bits get used or thrown out?

In general, SAML itself defines nothing related to TrustManagement. Mechanisms like SSL/TLS and XMLSignature, along with others, are spelled out as viable (and in some cases required) approaches to securing SAML profiles, but there are no guidelines or rules for how to make them usable and expose the configuration of policies and key management to the deployer. (In fact, absolutely **nothing** in the standards world addresses this. Makes writing this stuff fun.)

TrustManagement is "bootstrapped" in the software using MetaData. That is, MetaData is implicitly trusted once a lookup is successful, and it provides the rules that drive the various TrustEngines provided with the software. There is a distinct API that can supply alternate TrustEngines, and they may choose to implement other mechanisms for obtaining such rules.