TrustEngine

A trust engine is a component responsible for answering two types of runtime questions:

- Is a signature created by a given entity valid?
- Is a security credential presented by an entity (e.g. for SSL/TLS) valid?

At any given time that one of these question is asked, the issuer of the message or presumed owner of the credential must be known. Going further, the "role" in which the entity is acting must also be known, to enable entities to use different keys when acting in different ways. This breakdown aligns with the SAML 2.0 Metadata design, which assigns key information to entity roles, not directly to entities.