

ProtoGENI Security Architecture

March, 2011

Darwin Witt

The design of the ProtoGENI security architecture is based on the knowledge that all entities that ProtoGENI will authenticate have unique global identifiers. ProtoGENI implements a single Public Key Infrastructure (PKI) server which covers authentication of all registries, aggregates and principals. This PKI provides all necessary certificates, and allows verification to be done using a limited number of root certificates.

The ProtoGENI global identifier (GID) consists of a unique user identifier (UUID) and Human Resolvable Name (HRN) all implemented in the DN of the SSL certificate. The SSL certificate is issued by the home Emulab server that authenticates the entity in GENI. The DN also includes the email address of the users. Despite the existence of UUIDs, ProtoGENI has moved to URN-based identifiers in order to separate identification from authentication. Each principal actor in the ProtoGENI control framework has been issued a unique URN. The authority that issued the URN may issue certificates binding authentication material to that URN.

Authorization in the ProtoGENI system is initiated by the exchange of credentials that facilitate resource authorization and access control by aggregates. The Public Key Infrastructure (PKI) that is used to authenticate principals provides all of the keys and other structure to sign and verify credentials during this process.