

Introduction

POLICY AUTHORITY PROCEDURES

For the Arizona Electronic Signature Infrastructure (AESI)

Version 1.00

September 1999

1. Introduction

The Policy Authority (PA) is responsible for defining and managing the Arizona Electronic Signature Infrastructure (AESI). The Arizona Electronic Signature Infrastructure consists of all of the State of Arizona's collections of electronic signing mechanisms and the entities and tools that enable the valid use of these forms of signatures. [This conception of the infrastructure is modeled after the IETF conception of PKI.¹][note there are multiple collections]

While there will undoubtedly be a rapidly evolving electronic signature technology, the Policy Authority expects that the underlying business processes and legal principals will be relatively constant across the variety of technical solutions that come to be used. The procedures defined within this document shall govern the full range of electronic signature solutions that evolve within the AESI.

The business process roles involved are defined in the AESI Definitions and Acronyms (see appendix). They broadly follow the roles defined in the CARAT *Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates*². The roles include Service Provider roles such as *Issuer*, *Certificate Manufacturer*, *Registrar*, and *Repository* and End Entity roles such as *Subscriber* and *Relying Party*. These roles may be performed by a variety of parties, e.g. the roles of *Issuer*, *Certificate Manufacturer*, *Registrar* are often performed by a party known as a *Certificate Authority (CA)*, and *Repository* is sometimes performed by the CA and sometimes by a party known as a *Repository Authority (RA)*. There are several ways of assigning roles to parties, however it is the role, not the party, that is important.

An electronic signature within the AESI is a contractual agreement between the subscribing party and a Issuer, such that the mechanism is a certificate issued to the subscriber. Such certificates point to a Certificate Policy (CP) that outlines the "boundaries and limitations" of the certificate. A Certificate Policy creates a "specific" Electronic Signature Infrastructure (ESI) within the global AESI setting. The Policy Authority shall define the responsibilities of the roles necessary in the Certificate Policies within the AESI.

Only digital signature technologies are presently recognized within Arizona Law, rules and standards. This will evolve. The basic business processes and legal principles are expected to remain the same. Thus as the technology may change, yet the underlying infrastructure shall remain relatively consistent. To accommodate, each particular technology or unique business process simply has one or more specific Certificate Policies. These specific groups of CP define the "specific" ESI within the global AESI.

¹ "A collection of certificates, with their issuing CA's, subjects, relying parties, RA's, and repositories, is referred to as a Public Key Infrastructure, or PKI." [from the IETF draft *Internet X.509 Public Key Infrastructure PKIX Roadmap* (draft-ietf-pkix-roadmap-02.txt)]

² Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates drafted by the Certification Authority Rating and Trust (CARAT) Task Force of the National Automated Clearing House Association (NACHA)..