



High performance. Delivered.

PKI Implementation in the Real World

Lessons Learned



Client CA Implementation

One of our current Government clients has implemented a Certificate Authority to issue PKI certificates for Federal Employees at participating Agencies.

- Recently, they asked us to help them document and update their processes, and help to expand their business.
- We can use their example to understand a real world implementation and gather some lessons learned.
- We will call this client “US Certificate Authority,” or USCA.

Glossary

Public Key Crypto – key pairs used to encrypt/decrypt or sign/verify

Certificate – a digital method of binding a key pair or pairs to a specific identity

Certificate Authority – the system that securely creates the certificates

Public Key Infrastructure – the whole system of creating, issuing, managing, utilizing and revoking certificates