NHIN Digital Certificates

Version 1.0

Last update: April 28, 2010

NHIN Digital Certificates

This paper answers questions as to the types and uses of digital certificates for the Nationwide Health Information Network (NHIN). NHIN digital certificates are managed Public Key Infrastructure (PKI), establishing security for the exchange of health care information using NHIN standards, services and policies. Without getting overly complex, certificates are necessary to verify a participant's identity to an end user and make it possible to encrypt the communication between two hosts. More information about PKI can be found in Wikipedia.

There are three different types of certifications defined today for the NHIN program:

1. ***Development certificate*** for unit and integration testing.
2. ***Validation certificate*** for NHIN validation testing; required to participate in the NHIN Exchange.
3. ***Production certificate*** for access to the NHIN Exchange.

The Office of the National Coordinator for Health IT (ONC) does not provide development certificates. ONC recommends that organizations either create a self-signed certificate or use a free certificate from a certificate provider.

- A *self-signed certificate* is an identity certificate that is signed by its own creator. This means self-signed certificates are the same as signed versions except for the fact that a Certificate Authority (CA) doesn't stamp it with their approval; instead the creator stamps it with their own approval.
- *A free certificate* can be acquired using organizations such as caCERT (http://www.cacert.org), or organizations ready to offer a Class 1 (limited level of security) certificate that will meet development needs. Additionally, best of the breed certificate providers such as VeriSign (http://www.verisign.com) also offer a trial version certificate for short durations which may suffice for the purpose of development.

ONC provides validation and production certificates. These certificates are issued by a third party CA, managed by ONC. These certificates are valid for a one-year period, after which they will have to be reissued. This one-year period is the best practice. It maximizes the certificate's security as the longer a public/private key pair is in use, the greater the chances are that the keys can be compromised.

Validation/Production Certificate Issuance Workflow

Prerequisites

- Validation Certificate
  - NHIN Exchange Application submitted and accepted by ONC
- Production Certificate
  - Approved for membership in the NHIN Exchange
  - Local Registry Authority (LRA) executed, notarized, and submitted to ONC

Activities

1. Organization completes a certificate request form and submits it to the NHIN Implementation Team.
2. NHIN Implementation Team logs into the Certificate Authority (CA) and creates an account for the Organization.
3. NHIN Implementation Team sends two Emails to the Organization:
   a. First Email provides the CA URL log on information and instructions (including a Reference Number).
   b. Second Email provides the Organization's Authorization Number.
4. Organization receives the Emails, logs into the CA account, and requests a digital certificate.
5. Organization receives the digital certificate from CA and installs the digital certificate on the host machine.

For more information, contact the NIHN Implementation Team at nhin@hhs.gov.