CHAPTER 21

ACQUIRING AND MANAGING DIGITAL CERTIFICATES

PURPOSE:

This chapter establishes the minimum requirements and standards for acquiring and managing digital certificates within the Department's information technology infrastructure.

AUTHORITY:

Sections 20.23(3)(a), and 334.048(3) Florida Statutes (F.S.)

REFERENCES:

Sections 668.006, 668.50(h), and 668.003(1)(a)-(d), Florida Statutes
Chapter 74-2 Florida Administrative Code (F.A.C.)
NIST Special Publication 800-63-3
Rule 60L - 36.005, F.A.C.
Procedure No., 250-012-011, Disciplinary Actions
Chapter 815, Florida Statutes
Chapter 23 of this manual

SCOPE:

The provisions of this chapter apply to all District and Central Office units within the Department. This chapter establishes the minimum requirements and standards for acquiring and managing digital certificates. District and Central Office units that employ the use of digital certificates shall implement an appropriate local procedure establishing unit specific processes and requirements. Any local procedures established shall neither supersede nor abridge the minimum requirements and standards within this chapter.

BACKGROUND:

In accordance with ***668.003, F.S.***, "a "Certificate" means a computer-based record which: identifies the certification authority, identifies the subscriber, contains the subscriber's public key, is digitally signed by the certificate authority," digital certificates may streamline processes, reduce paper printing, and create efficiencies within the Department. As demand for digital certificates increases within the Department, it becomes necessary to establish minimum requirements and standards for acquiring and managing digital certificates.

21.1 Procurement of Digital Certificates

21.1.1 Procuring Digital Certificates

To the extent possible, the procurement of digital certificates shall be centralized and shall be processed through the Office of Information Technology (OIT). The centralization of the procurement of digital certificates enables the Department to achieve cost savings through volume pricing. Requests to procure digital certificates shall be submitted by the requesting office through the ***Automated Access Request Form System (AARF)***. Upon approval of the ***access request***, OIT shall procure, if necessary, the digital certificate vouchers (generally new certificates) and/or order numbers (generally certificate renewals) in accordance with the provisions of the ***Procurement of Commodities and Contractual Services Procedure, Topic No.: 375-040-020.*** Upon the acquisition of the digital certificate voucher/order number, OIT shall distribute instructions on how to ~~obtain~~ redeem the voucher directly to the requestor. Digital Certificate renewals for existing users should be requested, by that individual, via the ticketing system of the FDOT Service Desk. Upon notification of the need for renewal, OIT shall distribute instructions on how to validate the renewal along with a pre-paid order number. Instructions for either a new digital certificate or the renewal of an existing digital certificate is meant for the approved individual only. Copying, replicating, forwarding or sharing instructions containing voucher and/or order numbers is not allowed. For requesting certificates that are not on the approved list, refer to ***Chapter 23, section 23.2.1.***

21.1.2 Eligible Digital Certificate Users

Only approved FDOT employees and OPS employees are eligible for the installation and use of FDOT procured digital certificate vouchers and/or order numbers. Contractors are not eligible for FDOT procured digital certificates even if it is a requirement of their duties.

21.1.3 Approved Digital Certificate Vendors

The Department shall procure digital certificates from only those vendors whom the Department has approved. An authorized vendor, also called a Certified Service Provider (CSP), must adhere to the records retention requirements specified in ***NIST Special Publication 800-63-3***. The OIT shall maintain a standards list of those vendors whom the Department has approved as both reputable and secure. In the event that a requesting office has identified a need to utilize a vendor not on the Department's standards list, the requesting office shall submit a request for exception to standard, along with a justification, within the ***Information Resource Request System***. The Department's Information Security Manager (ISM) shall be assigned delegated review for the exception to standard, and the request must receive ISM approval prior to procurement.

21.1.4 Digital Certificate Accountability

The Office of Information Technology is responsible for the timely issuance of digital certificate vouchers, and the timely revocation of digital certificates. Cost Center Managers are responsible for the timely submittal of AARF requests for those individuals who no longer require a digital certificate assignment. Digital Certificate holders are responsible for the timely renewal of the digital certificates.

21.2 Implementing Digital Certificates

District and Central Office units shall create and submit a ***Digital Certificate Security Assessment*** to the Department's ISM for review and approval prior to the implementation of digital certificates within the specific District or Central Office unit. The Department's ISM shall retain all approved Digital Security Certificate Assessments for historical and auditing purposes.

21.2.1 Digital Certificate Security Assessments

At a minimum, ***Digital Certificate Security Assessments*** shall include the following information:

a) Major application of the certificate (describe the use of the certificate)
b) Assurance level required (Level 1 through Level 4)
    a. For digital certificates used for digital signatures, the digital certificate shall be at least an Assurance Level 3

c) Senior Management Service (SMS) or Select Exempt Service (SES) level Sponsor approving the use of digital certificates
d) Initial number of digital certificates needed

21.3 Managing Digital Certificates

21.3.1 Installation of Digital Certificates

Only the user to whom the digital certificate is issued (digital certificate holder) shall perform the initial installation of the digital certificate. In some cases, OIT support staff (either locally or via remote software tool) may need to assist in the installation by providing Administrative Rights that will allow the technology resource to accept the download and installation. Department purchased digital certificates shall only be installed on Department owned or leased information technology resources. Certain certificates may be transferable from one information technology resource to another.

21.3.2 Removal of Digital Certificates

In the event a digital certificate holder no longer requires a digital certificate, the digital certificate assigned to the digital certificate holder shall be removed from all information technology resources within two business days, starting from the first full business day the digital certificate holder no longer requires the digital certificate. Removal of the digital certificate means the purging of the digital certificate from all information technology resources such that there is assurance that the certificate may not be reconstructed using normal system capabilities. Further, in the event a digital certificate holder is assigned a new workstation and still has a need for a digital certificate, and a digital certificate is installed on the digital certificate holder's original workstation, the digital certificate shall be exported from the digital certificate holder's original workstation, and installed on the new workstation. Once the digital certificate is installed on the new workstation, the digital certificate shall be purged from the original workstation such that there is assurance that the certificate may not be reconstructed using normal system capabilities.

21.3.3 Digital Certificate Application Area

To the extent possible, digital certificates shall only be used for highly specified purposes. Digital certificates shall not be used for purposes other than those stated in the ***Digital Certificate Security Assessment***. District or Central Office units that identify the need for more than one application area for digital certificates shall submit a ***Digital Certificate Security Assessment*** for each major application of the digital certificates within the specified unit. If the need for using digital certificates across

multiple application areas is identified upon the initial implementation of digital certificates within the specified unit, the unit may incorporate all application areas into one ***Digital Certificate Security Assessment***, so long as the ***Digital Certificate Security Assessment*** satisfies the requirements specified in ***section 21.2.1 of this Chapter*** for each application area.

21.4 Compliance

Misuse or abuse of digital certificates is subject to the Department's disciplinary standards, up to and including immediate dismissal, civil penalties, or criminal penalties. Refer to the Department's ***Disciplinary Standards*** contained in ***Rule 60L-36.005, F.A.C.,*** and the ***Disciplinary Action Procedure, Topic No.: 250-012-011***. Failure to comply with related department policies, procedure, and standards may lead to termination of contracts for contractors, partners, consultants and other entities that provide service to the Department. Furthermore, pursuant to ***Chapter 815, F.S., Computer Related Crimes***, all individuals who violate these related statutes, rules, policies, procedures, and standards, are subject to possible legal (civil, or criminal, or both) prosecution. The appropriate use of digital certificates is governed via related Florida Statutes, Florida Administrative Code, and Department policies and procedures, especially ***Security and Use of Digital Certificates*** found in ***Chapter 23*** of ***this Manual***.

TRAINING:

None Required.

FORMS:

None Required.