CHAPTER 21

SECURITY AND USE OF CERTIFIED DIGITAL CERTIFICATES

PURPOSE:

This chapter establishes the minimum requirements and standards for acquiring, managing, and using certified 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 60GG-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

SCOPE:

The provisions of this chapter apply to all Department Office units. Department Office units that employ the use of certified 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:

Pursuant to Florida law, an electronic signature "means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record," section ***668.50(2)(h), F.S***. A certified digital certificate "means a computer-based record which: identifies the certificate authority,

identifies the subscriber, contains the subscriber's public key, [and] is digitally signed by the certification authority," section ***668.003(1)(a)-(d), F.S.***

Certified digital certificates may streamline processes, reduce paper printing, and create efficiencies within the Department. As demand for certified digital certificates increases within the Department, it is necessary to establish minimum requirements and standards for acquiring, managing, and using certified digital certificates.

21.1 Use of Certified Digital Certificates

21.1.1 The use of certified digital certificates and electronic signatures within the Department shall be governed in accordance with the provisions of Department policies, procedures, handbooks, and manual chapters governing such use, as well as Florida law. Unless otherwise provided by law, an electronic signature may be used to sign a writing and shall have the same force and effect as a written signature. If Department policy or Florida law requires the notary of a signature or record, the authorized and legal notary may use an electronic signature to satisfy the notary requirement so long as all legally required information is attached to or logically associated with the signature or record.

21.1.2 The use of certified digital certificates and electronic signatures shall be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices. ***This chapter*** establishes the procedural requirements for the acquisition, management, and revocation of certified digital certificates, including those certified digital certificates used for electronic signatures.

21.1.3 Certified digital certificates shall only be used by the individual to whom the certified digital certificate is assigned (the certified digital certificate holder). Certified digital certificate holders may not grant the use of his or her assigned certified digital certificate for use by others, including delegates. Delegates authorized to affix electronic signatures on behalf of a delegator shall have assigned to him or her, his or her own certified digital certificate for that stated purpose. Further, delegates shall refuse the receipt of a certified digital certificate that is not specifically assigned to him or her.

21.1.4 Certified digital certificate holders shall not use certified digital certificates for other than the certificate's stated or implied purpose.

21.1.5 The implementation of a certified digital certificate for specific processes requires Senior Management Service (SMS) or Traditional Select Exempt Service

(SES) level approval. Further, third parties must agree to conduct business transactions via an electronic means prior to the implementation of certified digital certificates. At any time, any party engaged in electronic transactions may withdraw previously provided agreement to conduct business electronically. “Whether the parties agree to conduct transactions electronically is determined from the context and surrounding circumstances, including the parties’ conduct,” section ***668.50(5)(b), F.S.***

21.2 Procurement of Certified Digital Certificates

21.2.1 Procuring Certified Digital Certificates

To the extent possible, the procurement of certified digital certificates shall be centralized and shall be processed through the Office of Information Technology (OIT). The centralization of the procurement of certified digital certificates enables the Department to achieve cost savings through volume pricing. Requests to procure certified 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 certified digital certificate vouchers (generally new certificates) and/or order numbers (generally certificate renewals) in accordance with the provisions of the ***Commodities and Contractual Services Procurement Manual, Topic No.: 375-040-020.*** Upon the acquisition of the certified digital certificate voucher/order number, OIT shall distribute instructions on how to 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 certified digital certificate or the renewal of an existing certified 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 ***section 21.2.3.***

21.2.2 Eligible Certified Digital Certificate Users

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

21.2.3 Approved Certified Digital Certificate Vendors

The Department shall procure certified 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***. OIT shall maintain a list of authorized vendors for certified digital certificates. This list shall be incorporated into the Department's Standards List, as specified in ***Chapter 8 of this Manual***. 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.

21.3 Implementing Certified Digital Certificates

Department Office units shall create and submit a ***Certified Digital Certificate Security Assessment*** to the Department's ISM for review and approval prior to the implementation of certified digital certificates for an application or process. The Department's ISM shall retain all approved Certified Digital Security Certificate Assessments for historical and auditing purposes.

21.3.1 Certified Digital Certificate Security Assessments

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

1. Major application of the certificate (describe the use of the certificate)
2. Assurance level required
    a. For certified digital certificates used for digital signatures, the certified digital certificate shall be at least an Identity Assurance Level 2 (IAL2) and Authenticator Assurance Level 2 (AAL2)
3. Senior Management Service (SMS) or Select Exempt Service (SES) level Sponsor approving the use of certified digital certificates
4. Initial number of certified digital certificates needed

21.3.2 Certified Digital Certificate Application Area

To the extent possible, certified digital certificates shall only be used for highly specified purposes. Certified digital certificates shall not be used for purposes other than those stated in the ***Certified Digital Certificate Security Assessment***. Department Office

units that identify the need for more than one application area for certified digital certificates shall submit a ***Certified Digital Certificate Security Assessment*** for each major application of the certified digital certificates within the specified unit. If the need for using certified digital certificates across multiple application areas is identified upon the initial implementation of certified digital certificates within the specified unit, the unit may incorporate all application areas into one ***Certified Digital Certificate Security Assessment***, so long as the ***Certified Digital Certificate Security Assessment*** satisfies the requirements specified in ***section 21.3.1 of this Chapter*** for each application area.

21.4 Managing Certified Digital Certificates

21.4.1 Requesting Certified Digital Certificates

Users requiring a certified digital certificate shall request the certified digital certificate via the AARF System. Upon the approval of the AARF request, it is the responsibility of the Enterprise Technology Services and Support team to acknowledge or reject the request, and to assist the user with obtaining the required certified digital certificate.

21.4.2 Installation of Certified Digital Certificates

Only the user to whom the certified digital certificate is issued (certified digital certificate holder) shall perform the initial installation of the certified 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 certified 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.

21.4.3 Removal of Certified Digital Certificates

Digital certificates shall be removed from all information technology resources within two business days of a person no longer requiring the certificate. Removal of the certified digital certificate means the purging it from all information technology resources such that there is assurance that the certificate may not be reconstructed using normal system capabilities. When a certified digital certificate holder is assigned a new workstation and still has a need for a digital certificate the certified digital certificate shall be exported from the original workstation, and installed on the new workstation and purged from the original workstation such that there is assurance that the certificate may not be reconstructed using normal system capabilities.

21.4.4 Revoking and Purging Certified Digital Certificates

Regardless of cause, when a certified digital certificate holder no longer requires access to an assigned certified digital certificate, the user's Supervisor shall ensure that an AARF Request is submitted to request the removal of the certified digital certificate. Upon receipt of the approved AARF Request, the Enterprise Technology Services and Support Team shall submit a request to the Certificate Authority to revoke the certificate.

Revoked certified digital certificates shall be purged from all systems upon which the certificate is installed in accordance with the requirements established in ***section 21.4.3 of this Chapter.***

21.4.5 Backup of Certified Digital Certificates

Backup of the certified digital certificate is the responsibility of the certified digital certificate holder. The backup file shall be placed on a Department network share to which the holder has access. The backup of the certified digital certificate shall be password protected. The certified digital certificate holder shall protect the backup file and associated password from unauthorized access and disclosure.

21.5 Certified Digital Certificate Accountability

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

Certified Digital Certificate holders are responsible for the following:

1) Protecting the certified digital certificate from unauthorized use

2) Using the certified digital certificate for only the stated or implied use

3) Protecting any passwords associated with the certified digital certificate from unauthorized disclosure

4) Assuring that the certified digital certificate assigned to a certified digital certificate holder is only installed and used on Department owned or leased information technology resources

5) Timely notification of the need to renew an assigned certified digital certificate to the appropriate certified digital certificate coordinator

6) Immediately reporting suspected breaches of security as specified in ***Chapter 1 of this Manual***

7) Backing up the certified digital certificate as specified in section ***21.5 of this Chapter***

8) Timely submittal of an Automated Access Request Form requesting the revocation of the certified digital certificate once certified digital certificate is no longer needed.

21.6 Compliance

Misuse or abuse of certified 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.

TRAINING:

None Required.

FORMS:

None Required.