Office of the Chief Information Officer Directive: IT 10.09	Issued: 04/2019 Last
Chapter: Network Security	Review: 01/2024
Subject: **ELECTRONIC COMMERCE**	

1 DIRECTIVE

1.01 All electronic commerce applications that rely on messages exchanged across a public network must provide security controls for meeting the following security requirements:

- Privacy and confidentiality. Access to the information for the messages comprising an electronic transaction must be restricted to authorized parties only.
- Integrity. Each message must be protected against alteration and tampering with while in transit from the sending party to the receiving party. Any such unauthorized alteration must be identified.
- Authentication. Both parties to each transaction must provide verifiable identification credentials for each message.
- Non-repudiation. Neither party to a completed electronic transaction can disclaim their role in the transaction.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that all electronic commerce transactions executed through a public network respect customer privacy and confidentiality, ensure the accuracy and integrity of financial transactions, authenticate all parties to a transaction, and prevent repudiation for a completed transaction.

3 SCOPE

3.01 This directive applies to all applications used to conduct financial transactions on a public network, including email.

4 RESPONSIBILITY

4.01 **IT Planning** is responsible to ensure that an appropriate infrastructure (i.e., both hardware and software) is established to support the controls required for electronic commerce.

4.02 **IT Application Development** and **IT Technical Support** are responsible to ensure that all e-commerce applications use the company-sponsored e-commerce infrastructure.

5 DEFINITIONS

5.01 "**Public network**" is any communications path that provides unrestricted access to any member of the public. This includes the Internet and all wireless communication systems.

5.02 "**PKI**" (**Public Key Infrastructure**) is a framework for exchanging information securely using encryption methods based on public key cryptography, an encryption method that uses encryption key pairs—a public key and a private key—to protect messages sent between two parties. In this scheme, the sender of a message uses the intended recipient's public key to encrypt the message. The recipient's matching private key is the only key that can decrypt the message.

5.03 "**Message hashing algorithm**" is a formula for computing a single number (the "hash number") from a larger message or text collection such that any change in the original message is likely to change the value of the corresponding hash number.

5.04 "**Digital signature**" is an electronic signature that may be used to authenticate the identity of a message sender. A digital signature cannot be imitated by a would-be impersonator and can be automatically time-stamped. By incorporating an encrypted message hash in the signature, it can also be used to guarantee that the sender's original message has not been altered during transmission and prevent later repudiation of the message by the sender.

5.05 "**Digital certificate**" is an electronic identifier used to establish the certificate owner's credentials on the Internet. It is issued by an independent certification authority (CA) associated with specific security purposes (such as commercial applications and government agency interactions). Examples of well-known commercial CAs are GeoTrust, GlobalSign, Thwarte and VeriSign Inc.

6 RELATED DIRECTIVES

OCIO IT 3.02 – Application Development and Implementation

OCIO IT 9.06 – Data Encryption