**Section 105.10 Scope and Definitions**

a) The purpose of this Part is to provide maximum flexibility to the implementation of digital signature technology, under the Electronic Commerce Security Act [5 ILCS 175], for State agencies and entities that do business with the State. The Department of Central Management Services serves as the single certification authority that may issue certificates to State agencies and as the primary certification authority that may issue certificates to persons, including non-State agencies, conducting business or other transactions with State agencies.

b) For the purposes of this Part, and unless the context expressly indicates otherwise, definitions are as follows:

"Act" means the Electronic Commerce Security Act [5 ILCS 175].

"Applicant" means a person conducting business or other transactions with a State agency that seeks certification of a security procedure by CMS, the State Certification Authority.

"Asymmetric Cryptosystem" means a computer-based system capable of generating and using a key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

"Certificate" means a record that, at a minimum:

identifies the certification authority issuing it;

names or otherwise identifies its subscriber or a signature device or electronic agent under the control of the subscriber;

contains a public key that corresponds to a private key under the control of the subscriber;

specifies its operational period; and

is digitally signed by the certification authority issuing it.

"Certification" or "Certify" means validation of compliance with the requirements of Section 105.200 of this Part.

"Certification Authority" or "CA" means the person or entity that authorizes and causes the issuance of a certificate. For purposes of this Part, the Department of Central Management Services is the CA.

"Certification Practice Statement" or "CPS" is a statement created by CMS, with the advice of the Policy Authority, that specifies the policies or practices that CMS employs in issuing, managing, suspending, and revoking certificates and providing access to them.

"Certificate Policy" or "CP" is a statement published by CMS, with the advice of the Policy Authority, that specifies the policies utilized in operation of the Public Key Infrastructure.

"Department" or "CMS" means the Department of Central Management Services.

"Digital Signature" means a type of electronic signature created by transforming an electronic record using a message digest function and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key such that any person having the initial untransformed electronic record, the encrypted transformation, and the signer's corresponding public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial electronic record has been altered since the transformation was made. A digital signature is a security procedure.

"Director" means the Director of the Department of Central Management Services.

"Electronic" includes electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies.

"Electronic Record" means a record generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another.

"Electronic Signature" means a signature in electronic form attached to or logically associated with an electronic record.

"Foreign Public Sector CA" means a certification authority that is a public sector entity of any government other than the government of the United States, any of the several states of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the territories and possessions of the United States, or any political subdivision thereof.

"Key Pair" means, in an asymmetric cryptosystem, 2 mathematically related keys, referred to as a private key and a public key, having the properties that:

one key (the private key) can encrypt a message that only the other key (the public key) can decrypt; and

even knowing one key (the public key), it is computationally unfeasible to discover the other key (the private key).

"Local Registration Authority" or "LRA" is the entity appointed by CMS to authenticate for a CA the identification of applicants desiring to become subscribers under this Part.

"Message Digest Function" means an algorithm that maps or translates the sequence of bits comprising an electronic record into another, generally smaller, set of bits (the message digest) without requiring the use of any secret information, such as a key, so that an electronic record yields the same message digest every time the algorithm is executed using the electronic record as input, and it is computationally unfeasible that any 2 electronic records can be found or deliberately generated that would produce the same message digest using the algorithm unless the 2 electronic records are precisely identical.

"Non-State Agency" means a person other than a State agency that is a public sector entity of any government, including, without limitation, a unit of local government, school district or board of elections created by or pursuant to the statutes of the State of Illinois, or any officer, commissioner, administrative unit or corporate outgrowth of the public sector entity. A non-State agency shall be deemed to be a person conducting business or other transactions with a State agency for purposes of the Act and this Part if it seeks certification of a security procedure by CMS or is a foreign public sector CA that seeks recognition under Section 105.240 of this Part.

"Operational Authority" (see State Operational Authority).

"Operational Period" means the period that begins on the date and time a certificate is issued by a certification authority (or on a later date and time certain if stated in the certificate) and ends on the date and time it expires as noted in the certificate or is earlier revoked, but does not include any period during which the certificate is suspended.

"Person" means an individual, corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental instrumentality, State agency, non-State agency, or any other legal or commercial entity.

"Policy Authority" (see State Policy Authority).

"Private Key" means the key of a key pair used to create a digital signature.

"Public Key" means the key of a key pair used to verify a digital signature.

"Public Key Infrastructure" or "PKI" means a structure of hardware, software, people, processes and policies for creating a secure method for exchanging information based on public key cryptography.

"Qualified Security Procedure" means a security procedure that meets the criteria established under Section 105.210.

"Record" means information that is inscribed, stored, or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

"Registration Authority" or "RA" means CMS in its role of authenticating the identity of subscribers prior to the issuance of certificates, but does not issue or sign the certificates.

"Rekey" means the process of securely regenerating signing/verification and/or encryption/decryption keys.

"Revocation" or "Revoke" means a temporary, conditional, or permanent termination of a certification as provided under Section 105.230 of this Part.

"Security Procedure" means a methodology or procedure used for the purpose of verifying that an electronic record is that of a specific person or detecting error or alteration in the communication, content, or storage of an electronic record since a specific point in time. A security procedure may require the use of algorithms or codes, identifying words or numbers, encryption, answer back or acknowledgment procedures, or similar security devices.

"Signature Device" means unique information, such as codes, algorithms, letters, numbers, private keys, or personal identification numbers (PINs), or a uniquely configured physical device that is required, alone or in conjunction with other information or devices, in order to create an electronic signature attributable to a specific person.

"Signed" or "Signature" includes any symbol executed or adopted, or any security procedure employed or adopted, using electronic means or otherwise, by or on behalf of a person with intent to authenticate a record.

"State Agency" means and includes all officers, boards, commissions, courts, and agencies created by the Illinois Constitution, whether in the executive, legislative or judicial branch; all officers, departments, boards, commissions, agencies, institutions, authorities, universities, bodies politic and corporate of the State; and administrative units or corporate outgrowths of the State government that are created by or pursuant to statute, other than units of local government and their officers, school districts and boards of elections commissioners; all administrative units and corporate outgrowths of the above and as may be created by executive order of the Governor.

"State Certification Authority" or "State CA" means the Department of Central Management Services in its role as the single certification authority that may issue certificates to State agencies and as a certification authority that may issue certificates to persons, including non-State agencies, conducting business or other transactions with State agencies.

"State Operational Authority" or "State OA" means the Department of Central Management Services in its role of interpreting certificate policies, with the advice of the Policy Authority, developing and managing the Certification Practice Statement, maintaining the PKI and providing for the issuance of digital certificates.

"State Policy Authority" or "Policy Authority" or "PA" is an internal intergovernmental committee of State employees representing various State agencies who are appointed by the Director. The PA is responsible for recommending policies relating to the operation of the PKI operated by CMS and for advising CMS about the maintenance and enforcement of those policies.

"Subscriber" means a person who is the subject named or otherwise identified in a certificate, who controls a private key that corresponds to the public key listed in that certificate, and who is the person to whom digitally signed messages verified by reference to the certificate are to be attributed.

"Suspension" or "Suspend" means to temporarily suspend the operational period of a certificate for a specified time period or from a specified time forward.

"Trustworthy Manner" means through the use of computer hardware, software, and procedures that, in the context in which they are used:

can be shown to be reasonably resistant to penetration, compromise, and misuse;

provide a reasonable level of reliability and correct operation;

are reasonably suited to performing their intended functions or serving their intended purposes;

comply with applicable agreements between the parties, if any; and

adhere to generally accepted security procedures.

"Valid Certificate" means a certificate that a certification authority has issued and that the subscriber listed in the certificate has accepted.

"Verify a Digital Signature" means to use the public key listed in a valid certificate, along with the appropriate message digest function and asymmetric cryptosystem, to evaluate a digitally signed electronic record, so that the result of the process concludes that the digital signature was created using the private key corresponding to the public key listed in the certificate and the electronic record has not been altered since its digital signature was created.