DUPLICATE

SUKOHARJO REGENT
PROVINCE OF CENTRAL JAVA

REGULATION OF THE REGENT OF SUKOHARJO
NUMBER 47 YEAR 2021

ABOUT

APPLICATION OF ELECTRONIC CERTIFICATES IN ELECTRONIC-BASED GOVERNMENT SYSTEMS

BY THE GRACE OF GOD ALMIGHTY

SUKOHARJO REGENT,

Weigh :

a. that in order to realize electronic-based governance, it is necessary to manage and manage an electronic-based government system nationally;

b. that in order to protect information from the risk of data theft, data modification, data falsification and denial of transacted data as well as protection of electronic systems belonging to Electronics within the Sukoharjo Regency Government, adequate and reliable security measures are needed through a public key infrastructure cryptography scheme embodied in the form of use of Electronic Certificates;

c. that with the enactment of the Regulation of the Head of the National Crypto Agency Number 10 of 2017 concerning the Implementation of Electronic Certificates, it is necessary to implement Electronic Certificates in the Regions;

d. that based on the considerations as referred to in letters a, b, and c, it is necessary to stipulate a Regent Regulation concerning the Application of Electronic Certificates in an Electronic-Based Government System;

Remember :

1. Law Number 13 of 1950 concerning the Establishment of Regency Areas within the Province of Central Java;

2. Law Number 11 of 2008 concerning Information and Electronic Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843);

3. Law Number 23 of 2014 concerning Regional Government (State Gazette of the Republic of Indonesia of 2014 Number 244, Supplement to the State Gazette of the Republic of Indonesia Number 5587) as several times, most recently by Law Number 1 concerning Job Creation (State Gazette of the of Indonesia Year 2020 Number 245, Supplem State Gazette of the Republic of Indonesia

PARAF KOORDINASI
Kadis. Kominfo
Kabag. Hukum

6573);

4. Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (State Gazette of the Republic of Indonesia of 2018 Number 182);

5. Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (State Gazette of the Republic of Indonesia of 2012 Number 189, Supplement to the State Gazette of the Republic of Indonesia Number 5348);

6. Government Regulation Number 18 of 2016 concerning Regional Apparatus (State Gazette of the Republic of Indonesia of 2016 Number 114, Supplement to the State Gazette of the Republic of Indonesia Number 5887) as amended by Government Regulation Number 72 of 2019 concerning Amendments to Government Regulation Number 18 of 2016 concerning Regional Apparatus (State Gazette of the Republic of Indonesia of 2019 Number 187, Supplement to the State Gazette of the Republic of Indonesia Number 6402);

7. Regulation of the Minister for Empowerment of State Apparatus and Bureaucratic Reform Number 6 of 2011 concerning General Guidelines for Electronic Service Manuscripts in Government Agencies;

8. Regulation of the Minister of State Apparatus Empowerment Number 80 of 2012 concerning Guidelines for Manuscripts for Government Agencies (State Gazette of the Republic of Indonesia of 2013 Number 69);

9. Regulation of the Minister of Communication and Information Number 4 of 2016 concerning Information Security Management System (State Gazette of the Republic of Indonesia of 2016 Number 551);

10. Regulation of the Head of the National Archives of the Republic of Indonesia Number 6 of 2005 concerning Guidelines for the Protection, Security and Rescue of Vital State Documents/Archives;

11. Regulation of the National Crypto Agency Number 5 of 2014 concerning Cryptographic Algorithm Standards in Government Agencies (State Gazette of the Republic of Indonesia of 2014 Number 1862);

12. Regulation of the Head of the National Crypto Agency Number 10 of 2017 concerning the Implementation of Electronic Certificates (State Gazette of the Republic of Indonesia of 2017 Number 907);

13. Regulation of the National Cyber and Crypto Agency Number 2 of 2019 concerning the Organization and Work Procedure of the Electronic Certification Center (State Gazette of the Republic of Indonesia of 2019 Number 339);

PARAF KOORDINASI

Kadis. Kominfo	
Kabag. Hukum	

14. Regulation of the Head of the National Crypto Agency

Number 7 of 2017 concerning Guidelines for Implementing Encoding for Information Security in Regional, Provincial and Regency/City Governments (State Gazette of the Republic of Indonesia of 2017 Number 758);

15. Regulation of the National Crypto Agency Number 10 of 2017 concerning the Implementation of Electronic Certificates (State Gazette of the Republic of Indonesia of 2017 Number 907);

16. Sukoharjo Regency Regulation Number 12 of 2016 concerning Formation and Structure of Regional Apparatus (Sukoharjo Regency Gazette of 2016 Number 12, Supplement to Sukoharjo Regency Regional Gazette Number 236);

DECIDE

Set : REGIONAL REGULATION CONCERNING IMPLEMENTATION OF ELECTRONIC CERTIFICATES IN ELECTRONIC-BASED GOVERNMENT SYSTEMS.

PIG

GENERAL REQUIREMENTS

article 1

In this Regent Regulation, what is meant by:

1. The area is Sukoharjo Regency.
2. Regional Government is the Regent as an element of the Regional Government organizer who leads the implementation of government affairs which are the authority of the autonomous region.
3. The Regent is the Regent of Sukoharjo.
4. Regional apparatus is the supporting element of the Regent and the Regional People's Representative Council in the administration of Government Affairs which are the authority of the Region.
5. The Office of Communication and Informatics is the Office of Communication and Information of the Sukoharjo Regency.
6. Electronic-Based Government System, hereinafter abbreviated as SPBE, is the administration of government by utilizing information and communication technology to provide services to SPBE users.
7. The National Cyber and Crypto Agency is a Government Institution of the Republic of Indonesia which is tasked with implementing effective and efficient cyber security by utilizing, developing and consolidating all elements related to cyber security.
8. Encryption Security Manager is a Civil Servant who is fully appointed and responsible for the implementation of encryption security.

9. Encryption Security Implementation is a series of activities and preventive or countermeasures that are carried out in a planned, directed, and continuous manner to protect the continuity of encryption from all the essence of threats and disturbances in a single State Encryption System.

10. Encryption is an activity in the field of data/information security which is carried out by applying concepts, theories, arts and crypto sciences along with other supporting sciences in a systematic, methodological and consistent manner and is bound to the code of professional ethics.

11. Information is information, statements, ideas, and signs that contain values, meanings, and messages, both data, facts, and explanations that can be seen, heard, and read presented in various packages and formats in accordance with the development of information and communication technology. electronic or non-electronic.

12. Public Information is information that is generated, stored, managed, sent, and/or received by a public agency related to state administrators and administration and/or organizers and administration of other public bodies in accordance with the law as well as other information related to the interests of public.

13. Communication Relationship Pattern Password is a form or pattern of relationship between two or more entities in the process of sending and receiving information/messages/news safely using encryption.

14. Electronic Certificate is an electronic certificate containing an electronic signature and identity indicating the legal subject status of the parties in an electronic transaction issued by the electronic certificate operator.

15. Owner of Electronic Certificate is an individual or legal entity that has approved an agreement on the use of electronic certificate with the Regional Government.

16. Digital Certificate Authority, hereinafter abbreviated as OSD, is an electronic system that functions as an electronic certificate service at the National Cyber and Crypto Agency.

17. Electronic Certification Center, hereinafter referred to as BSrE, is a technical implementing unit for OSD organizers which is under and responsible to the National Cyber and Crypto Agency.

18. The Electronic Certificate Policy Committee, hereinafter abbreviated as KKSE, is the official responsible for determining a series of criteria or requirements in the process of issuing and managing Electronic Certificates, as well as determining the suitability of using Electronic Certificates in an electronic application/system.

19. Registration Authority, hereinafter abbreviated as OP, is the unit responsible for examining, granting approval or rejection of every request for issuance, renewal, and revocation of Electronic Certificates submitted by owners or prospective owners of OSD Lemsaneg Electronic Certificates.

20. Verifier is the head of field and section head w
responsible for examining each document requesti
issuance, renewal, and revocation of Electronic Cer

PARAF KOORDINASI	
Kadis. Kominfo	
Kabag. Hukum	

submitted by owners or prospective owners of OSD Lemsaneg Electronic Certificates.

21. Security Auditor is the person responsible for auditing the suitability and security of the BSSN OSD as well as the registration authority.
22. *Certificate Policy* , hereinafter abbreviated as CP, is the provisions and policies that regulate all parties related to the use of electronic certificates issued by BSrE.
23. *Certificate Practice Statement* , hereinafter abbreviated as CPS, is a statement regarding the procedures related to the issuance, use, regulation, withdrawal, and renewal of Electronic Certificates by BSrE.
24. Cryptographic key pairs are private and public keys that are associated with each other.
25. Information System is a set of tools and procedures that function to prepare, collect, process, analyze, store, display, announce, transmit and/or disseminate information managed within the Local Government Environment.
26. Electronic Transactions are legal acts carried out using computers, computer networks and/or other electronic media.
27. Electronic Document is any electronic information that is created, forwarded, sent, received or stored in analog, digital, electromagnetic, optical or similar forms that can be seen, displayed and/or heard through a computer or electronic system, not limited to writing, sound, letters. , signs, numbers, access codes, symbols or perforations that have meaning or significance or can be understood by people who are able to understand them.
28. Electronic Signature is a signature consisting of electronic information that is attached, associated or related to other electronic information that is used as a means of verification and authentication.
29. Private Key is one of the keys of a cryptographic key pair that is only stored and kept confidential by the user and is used to perform electronic signatures or to open messages encoded using the Public Key on the Electronic Certificate.
30. Public Key is one of the keys of a cryptographic key pair that is owned by certain parties and can be used by other parties to exchange information securely with the owner of the key.
31. *Passphrase/ Password* is a series of numbers and/or letters and/or certain characters used as an authentication tool to access private key pairs and Electronic Certification.
32. *Reverse Engineering* is a process of searching and discovering the technological systems, functions and operations that work behind an in-depth look at each structural component of the design or object under study.

Section 2

This Regent's Regulation is intended as a guideline Apparatuses in administering and using Electronic C information security in Electronic Transactions impl developed at SPBE within the Regional Government.

Article 3

This Regent Regulation aims to:

a. create a pattern of good and secure communication relations in electronic Transactions in Regional Apparatuses;

b. assist the Regional Apparatus in securing information belonging to the Regional Apparatus;

c. improve the performance of Regional Apparatus in the implementation of SPBE;

d. ensure the integrity and authenticity of information in order to ensure that the information is not changed/modified during storage and delivery;

e. guarantee *non* -repudiation and ensure that the owner of the information cannot deny that the information belongs to or has been authorized by him;

f. maintain the confidentiality of information that can only be accessed by authorized parties;

g. increase confidence in the implementation of SPBE; and

h. improve efficiency and effectiveness of government administration in public services through SPBE.

CHAPTER II

SCOPE

Article 4

The scope of this Regent Regulation includes:

a. administration of Electronic Certificates;

b. procedures for application, issuance, renewal and revocation of Electronic Certificates;

c. the benefits and functions of Electronic Certificates on SPBE;

d. verifier;

e. the validity period of the Electronic Certificate;

f. obligations and prohibitions for Electronic Certificate owners; and

g. penalty.

CHAPTER III

ELECTRONIC CERTIFICATE OPERATION

Part One

General

Article 5

The parties in the administration of electronic certificates consist of:

a. BSrE includes:
   1. KKSE;
   2. OP; and
   3. Security auditors.
b. Verifier; and
c. Electronic Certificate Owner.

The second part

BSrE

Article 6

The BSrE as referred to in Article 5 letter a is in charge of:

a. manage and issue Electronic Certificates used in electronic systems to fulfill electronic information security aspects in government agencies;
b. issue and ensure Electronic Certificates are in accordance with the provisions stipulated in the CP;
c. carry out OP and delegate to Electronic Certificate Owner agencies; and
d. revoke the OP status of the agency holding the electronic certificate if it does not carry out its duties and functions.

Article 7

(1) KKSE as referred to in Article 5 letter a number 1 is in charge of:
   a. compile and manage the CP OSD Lemsaneg from the electronic certification provider operated on the OSD Lemsaneg;
   b. ensure that all aspects of services, oper infrastructure as described in the CPS do carried out in accordance with the criteria s Lemsaneg CP OSD document;
   c. provide recommendations for the impleme operation of the electronic certification sys Lemsaneg OSD;
   d. formulating follow-up on the results of the auditor's assessment; and
   e. provide recommendations for the temporary cessation of Lemsaneg's OSD operations.

(2) In carrying out the tasks as referred to in paragraph (1), KKSE is authorized to provide guidance to the administration of electronic certificates.

Article 8

(1) The OP as referred to in Article 5 letter a number 2 is carried out by the BSrE and can be delegated to the agency that holds the Electronic Certificate.
(2) The delegation as referred to in paragraph (1) is carried out based on a feasibility test.
(3) OP as referred to in paragraph (1) must carry out its duties and functions.

(4) The duties and functions as referred to in paragraph (3) are based on the provisions stipulated in the CP.

(5) BSrE has the right to revoke the OP status of the agency holding the electronic certificate if it does not carry out its duties and functions.

Article 9

(1) The security auditor as referred to in Article 5 letter a number 4 carries out the audit process periodically.

(2) The audit process as referred to in paragraph (1) can be carried out by external parties.

Part Three

Verifier

Article 10

(1) Verification is carried out by the Department of Communication and Information.

(2) The verifier as referred to in paragraph (1) has the following duties and authorities:

a. perform identification and analysis of the need for electronic certificates;

b. develop or provide input to Regional Apparatuses to create systems/applications supporting the use of electronic certificates;

c. make recommendations on the use of electronic certificates and/or supporting applications for the use of electronic certificates;

conduct socialization and technical guidance related to the use of electronic certificates;

d. provide education to the owner of the electronic certificate which at least includes the rights, obligations and responsibilities, as well as the procedure for filing a complaint;

e. verify registration, renewal and revocation of electronic certificates; and

f. supervise and evaluate the use of Electronic Certificates.

(3) verifier as referred to in paragraph (1) shall prepare Standard Operating Procedures and conduct socialization to related parties.

Article 11

(1) Verifiers as referred to in Article 10 include :

a. Head of Coding and Statistics at the Department of Communication and Information; and

b. Head of the Password and Information Securit the Communications and Information Technolo

(2) verifier as referred to in paragraph (1) already has a Certificate and is appointed by the BSrE.

Part Four

Electronic Certificate Owner

Article 12

(1) Owners of Electronic Certificates as referred to in article 5 letter c consist of:

a. Government employees;

b. Village head; and

c. Village Apparatus.

(2) The Head of Regional Apparatus as referred to in paragraph (1) is required to have an Electronic Certificate.

Article 13

(1) The owner of the Electronic Certificate as referred to in article 12, must meet the requirements and criteria in protecting the Private Key and agree to the conditions for the use of the Electronic Certificate before the Electronic Certificate is issued.

(2) The requirements and criteria as referred to in paragraph (1) are further regulated in the CP.

CHAPTER IV

PROCEDURES FOR APPLICATION, ISSUANCE, RENEWAL AND REVOCATION OF ELECTRONIC CERTIFICATES

Part One

General

Article 14

The Electronic Certificate Ownership Process consists of:

a. Electronic Certificate application:

b. issuance of Electronic Certificates;

c. Electronic Certificate renewal; and

d. revocation of Electronic Certificate.

The second part

Application

Article 15

(1) Application for Electronic Certificates as referred to in Article 14 letter a, is a process of requesting Electronic Certificates submitted by Applicants for Electronic Certificates to the Head of the Office of Communication and Information Technology.

(2) The applicant as referred to in paragraph (1) includes:

a. Government employees;

b. Village head; and

c. Village Apparatus.

PARAF KOORDINASI

Kadis. Kominfo	
Kabag. Hukum	

Article 16

(1) The application as referred to in article 15 must cc

a. application letter for Issuance of Certificates;

b. photo of Electronic Identity Card;

c. selfie photo of the applicant;

d. *photocopy* and scan of Decision Letter of Appointment in the Last Position and/or Decision Letter of Last Promotion; and

e. *email* using mail@sukoharjokab.go.id .

(2) The Head of the Office of Communication and Information as referred to in Article 15 paragraph (1) submits an application for the issuance of Electronic Certificates to BSrE by completing:

a. application letter for Issuance of Certificates;

b. photo of Electronic Identity Card;

c. applicant's selfie;

d. *photocopy* and scan of Decision Letter of Appointment in Last Position and/or Decision Letter of Last Promotion;

e. *email* using mail@sukoharjokab.go.id ; and

f. letter of recommendation for the issuance of Electronic Certificate from the Office of Communication and Information Technology.

(3) BSrE issues a *link* containing an Electronic Certificate registration form for applicants to fill out *online* .

(4) The applicant re-sends the *link* of the electronic certificate registration form as referred to in paragraph (3) by giving the approval of the Electronic Certificate Owner Agreement through the OSD application.

Part Three

Publishing

Article 17

(1) Issuance of Electronic Certificate as referred to in Article 14 letter b, is the process of approval of application and signing of Electronic Certificate by BSrE;

(2) The issuance of the Electronic Certificate as referred to in paragraph (1) is carried out through an application provided by the BSrE;

(3) Issuance of Electronic Certificates in the form of extensions determined by BSrE.

(4) The extension as referred to in paragraph (3) is a *private key* .

(5) The Electronic Certificate as referred to in p
contains an Electronic signature in the form of t
and/or a picture of the BSrE and reads “this document has been signed electronically” by the owner of the electronic signature or according to the BSrE application.

Article 18

Electronic Certificates issued by BSrE become the property or rights of the Electronic Certificate Owners.

Part Four

Update

Article 19

(1) Renewal of Electronic Certificate as referred to in Article 14 letter c, is the process of making a new Electronic Certificate in the event that:

a. the period of use of the Electronic Certificate will expire;

b. the pair of Private Key and Electronic Certificate is damaged/inaccessible; and

c. forgot *password/passphrase.*

Article 20

(1) In the event that the period of use of the electronic certificate as referred to in Article 19 letter a is carried out no later than 3 (three) days before the period of use of the certificate ends.

(2) The application for renewal of the period of use of the electronic certificate as referred to in paragraph (1) must complete the following requirements:

a. show Electronic Certificate; and

b. recommendation from the Head of the Office of Communication and Information Technology.

Article 21

(1) In the event that the pair of Private Key and Electronic Certificate is damaged/inaccessible as referred to in Article 19 letter b, the owner of the Electronic Certificate shall submit the renewal.

(2) The application for renewal as referred to in paragraph (2) must complete:

a. Show Electronic Certificate;

b. Recommendation from the Head of the Ministry of Communication and Informatics; and

c. Reason for damage/inaccessibility ,

Article 22

password/passphrase as referred to in Article 19 letter c is forgotten , the Electronic Certificate revocation proc out.

Part Five

revocation

Article 23

(1) The revocation of the Electronic Certificate as referred to in Article 14 letter d, is the process of stopping the use of the Electronic Certificate by the BSrE.

(2) Electronic Certificate revocation can be done by:

a. application; or

b. without a request from the Electronic Certificate Owner.

(3) The application for revocation of the Electronic Certificate as referred to in paragraph (2) letter a shall be submitted by the

Owner of the Electronic Certificate to the Head of the Office of Communication and Information Technology.

(4) The application for Electronic Certificate Revocation as referred to in paragraph (3) must complete:

a. letter of request for revocation;

b. Decree of Appointment in Last Position for owners with mutations and rotations;

c. retirement decree for owners who are retiring; and

d. certificate of loss for the owner who has lost the Electronic Certificate.

(5) The revocation of the Electronic Certificate without the application as referred to in paragraph (2) letter b shall be made to the Owner of the Electronic Certificate who does not meet the requirements as the Owner of the Electronic Certificate as regulated in the CP.

(6) Owners of Electronic Certificates who do not meet the requirements as referred to in paragraph (5) include:

a. Electronic Certificate holder does not serve/transfer/rotate;

b. Owner of a pension Electronic Certificate; and

c. Lost Electronic Certificate.

CHAPTER V

BENEFITS AND FUNCTIONS OF ELECTRONIC CERTIFICATES ON SPBE

Article 24

Electronic Certificates are used in carrying out official duties, including:

a. administering electronic systems and transactions;

b. administering the Service Manuscript System electronically;

c. administer the application or information system determined and/or provided by the Office of Communication and Information;

d. provide services at other SPBE determined and/or provided by the Central Government and Regional Governments; and

e. issue other electronic documents using electronic applications and systems.

Article 25

Electronic Certificates function as:

a. electronic signature;

b. electronic document security; and

c. *mail* security .

CHAPTER VI

ELECTRONIC CERTIFICATE VALIDITY

Article 26

The Electronic Certificate is valid for 2 (two) years as of the date the Electronic Certificate is issued.

CHAPTER VII

OBLIGATIONS AND PROHIBITIONS FOR ELECTRONIC CERTIFICATE OWNER

Article 27

Owner of Electronic Certificate must:

a. maintain the security of the *passphrase/password* and the pair of Private Keys and Electronic Certificates owned;
b. provide correct information to the Office of Communication and Information;
c. apply for Electronic Certificate revocation, if you know or suspect that the Electronic Certificate owned is used by another person or there is misinformation or loss or leakage of private keys;
d. protect the confidentiality of the private key, *passphrase/password* or anything else used to activate the private key;
e. not modify, interfere with or *reverse-engineer* and attempt to divulge the security services provided by the Communications and Information Technology Service;
f. responsible for the use, storage, renewal and destruction of Electronic Certificates and private keys; and
g. immediately notify the Verifier if the owner finds out that the Electronic Signature creation data has been burglarized.

Article 28

Owners of Electronic Certificates are prohibited from:

a. provide electronic certificate *passwords/passphrases* to others;
b. hand over or authorize the use of electronic certificates to other people;
c. access a system to which they are not entitled; and
d. falsify the data on the requirements for the Certificate application.

CHAPTER VIII

PENALTY

Article 29

Every Electronic Certificate owner who does not carry out the obligations as referred to in Article 26 and/or violates the prohibition as referred to in Article 27 is subject to sanctions in the form of revocation of Electronic Certificates and/or sanctions in accordance with the provisions of the legislation.

CHAPTER IX

TRANSITIONAL TERMS

Article 30

Heads of Regional Apparatuses who already have electronic certificates prior to the issuance of this Regent Regulation, are still valid until their validity period expires.

CHAPTER X

CLOSING

Article 31

This Regent Regulation comes into force on the date of promulgation.

For public cognizance, ordering the promulgation of this Regent Regulation by placing it in the Sukoharjo Regency Regional Gazette .

Set in Sukoharjo
on October 1, 2021
BUPATI SUKOHARJO
ttd.

ETIK SURYANI

Promulgated in Sukoharjo
on October 1, 2021

REGIONAL SECRETARY
SUKOHARJO DISTRICT ,

signed.

WIDODO

REGIONAL NEWS SUKOHARJO REGENCY
YEAR 2021 NUMBER 48

PARAF KOORDINASI
Kadis. Kominfo
Kabag. Hukum