CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs) Introduction must include:
1) CA's Legal Name :
Ministry of the Interior and Safety (formerly, Ministry of the Interior)
2) Root Certificate using Algorithm RSA
3) MOIS used BR Version 1.5.1
4) URL for CPS : https://www.gpki.go.kr/upload/download/1.2-GPKI_CA CPS.pdf
5) Plan to update in our next version of CPS within October, 2017

BR Section Number	**List the specific documents and section numbers of those documents which meet the requirements of each BR section**	**Explain how the CA's listed documents meet the requirements of each BR section.**
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	CA CPS 1.	The CA CPS was revised on 29 September 2017 according to the Revision Table on the document. The document has been effective since the date when the document were published.
1.2.2. Relevant Dates Note the Compliance date for eachitem in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	CA CPS 1.5.4.	According to Section 1.5.4. of CA CPS, the head of Government Certification Management Authority accepts the revision of the document in case that a technical and/or administrative reason happens.

1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.	CA CPS 1.3.4.	According to CA CPS, the CA may have independent RAs for specific purposes. For example, the National Assembly may require an independent RA that has a separate system from CA's RA systems. Only specific government institutes can apply independent RAs that are not allowed to issue SSL certificates to any end users.
2.1. Repositories Provide the direct URLs to the CA's repositories	CA CPS 2.	For SSL certificates, relevant documents are published on the CA official website (www.gpki.go.kr).
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> Copy the specific text that is used into the explanation in this row. (in English)	CA CPS 2.3.	According to CA CPS, the CA publishes CPS and other relevant documents that are made or revised immediately. The CA publishes updated CRLs every day.
2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.	https://www.gpki.go.kr	Valid certificate: https://www.gpki.go.kr Revoked certificate: TBD (in October 2017) Expired certificate: TBD (in October 2017)

2.3. Time or frequency of publication Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.	CA CPS 2.3.	According to CA CPS, the CA publishes CPS and other relevant documents that are made or revised immediately. The CA publishes updated CRLs every day.
2.4. Access controls on repositories Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.	CA CPS 2.4.	Anyone can access CPS and relevant documents through the website.
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, indicate how your CP/CPS meets the requirements in this section of the BRs.	CA CPS 3.2.2 and 3.2.3	For SSL certificates, CA and/or RA verifies user identification such as domain names and email by WHOIS inquiry and an official documents issued by the government agency or institute.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, indicate how your CP/CPS meets the requirements in this section of the BRs.	CA CPS 3.1.6	MOI CA is owned and operated by the Government. MOI CA does not have Trade Marks.
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	CA CPS 3.1.1	MOI CA issued SSL certificates that contain KR countryName only.
3.2.2.4 Validation of Domain Authorization or Control Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs.	CA CPS 3.2.2	An applicant shall submit an official letter that ensures that the applicant is the government institute. MOI RA shall confirm the administrative standard code included into the official letter by the Government centralized administrative DB.

Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.		
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CA CPS 3.2.2	For SSL certificates, MOI RA confirms whether applicant's organzation name and email address are matched with them shown on WHOIS search.
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CA CPS 3.2.2	MOI RA verifies whether an applicant has an ownership and/or control of the email address indicated on the application form.
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CA CPS 3.2.2	RA conducts a phone-call verification to the applicant's organization.
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CA CPS 3.2.2	MOI RA verifies whether an applicant has an ownership and/or control of the email address indicated on the application form.
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CA CPS 3.2.2	MOI RA may request additional documents proving that an applicant has an ownership and/or control of the domain indicated on the application form.

3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	MOI CA doesn't support the Agreed-Upon Change to Website as one of verification methods.
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	MOI CA doesn't support DNS change as one of verification methods.
3.2.2.4.8 IP Address If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	MOI CA doesn't issue SSL certificates containing IP addresses.
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	MOI CA will provide test webpages for valid, revoked, and expired certificates in October 2017.
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	MOI CA doesn't support TLS Using a Random Number as one of verification methods.
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.	N/A	MOI CA doesn't issue SSL certificates containing IP addresses.

3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then indicate how your CA meets the requirements in this seciton of the BRs.	N/A	For wildcard certificates, domains are contained in SubjectCN and/or SAN of a certificate.
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	N/A	the Government centralized administrative DB is operated based on real-time. When the government reshuffle occurs, the government adjusts the DB contents within 1 week.
3.2.3. Authentication of Individual Identity	CA CPS 3.2.3	MOI RA shall confirm that the applicant should be registered into the Government centralized administrative DB. RA conducts a phone call and email check.
3.2.5. Validation of Authority	CA CPS 3.2.2	MOI RA shall verify whether the administrative code on the official letter to be submitted as an identification document must be matched with the Government centralized administrative DB.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CA CPS 3.2.6	MOI CA doesn't support any interoperability regarding SSL certificates.
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CA CPS 4.1.1	Only government officials and/or institute can apply SSL certificates to MOI CA. MOI CA doesn't issue any certificates to an applicant who is not identified according to CPS 3.2.4.

4.1.2. Enrollment Process and Responsibilities	CA CPS 4.1.2	MOI RA is responsible for checking whether the application information is accurate.
4.2. Certificate application processing	CA CPS 4.2	Certificate application processing is described on CPS 4.2
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.	CA CPS 4.2.1	All applicants must submit the official letter containing domain information to be applied. The official letter shall be signed or sealed by the principle, president, or representative of the government institute.
4.2.2. Approval or Rejection of Certificate Applications	CA CPS 4.2.2	MOI CA and/or RA may refuse a certificate application that has inaccurate and insufficient information. The return of an official letter by MOI CA may be used as a method of refusal notice.
4.3.1. CA Actions during Certificate Issuance	CA CPS 4.3.1	CA conducts the below activities while on issuance. - check whether an applicant works at a government institutes - check whether an applicant is identified - check whether an applicant has the ownership/control of the domain - check whether an CSR (PKCS#10) is correct.
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	CA CPS 4.9.1	MOI CA or RA revokes subscriber certificates as one of the below reasons: - subscriber requests to revoke his certificate - CA or RA recognizes that a subscriber has got an issued certificate by incorrect procedure. - CA or RA recognizes that an subscriber's private key is compromised or suspicious to be compromised.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	CA CPS 4.9.1	MOI CA or RA revokes CA certificates as one of the below reasons: - CA or RA recognizes that a CA's private key is compromised or suspicious to be compromised.
4.9.2. Who Can Request Revocation	CA CPS 4.9.2	According to CPS 4.1.1, only application institute or the Certificate Authorities accredited by the Ministry of Ministry of the Interior can request certificate revocation.
4.9.3. Procedure for Revocation Request	CA CPS 4.9.3	Subscriber can directly revoke his valid certificate at the official CA website. Or subscriber can request the certificate revocation by sending an official letter to CA. MOI RA may request certificates revocation to CA when government reshuffle occurs.
4.9.5. Time within which CA Must Process the Revocation Request	CA CPS 4.9.5	MOI CA and/or RA revokes SSL certificate within 24 hours after request.
4.9.7. CRL Issuance Frequency	CA CPS 4.9.7	CA issues CRLs every day (within 24 hours).
4.9.9. On-line Revocation/Status Checking Availability	CA CPS 4.9.9	OCSP for SSL certificate: http://ssl-ocsp-gov.gpki.go.kr:8100

4.9.10. On-line Revocation Checking Requirements Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.	CA CPS 4.9.10	A certificate verifier must validate the certificate using OCSP. The OCSP server accepts a GET Method HTTP request from the OCSP validation requestor.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	CA CPS 4.9.11	MOI CA supports SCVP (Server Based Certification Validation Protocol).
4.10.1. Operational Characteristics	CA CPS 4.10.1	The certificate status can be checked with the certificate revocation list and the real-time certificate status confirmation service.
4.10.2. Service Availability	CA CPS 4.10.2	The Certificate Status service is provided without a 24x365 interruption unless there is a planned interruption.
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS	CA CPS 5	There is 5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS on CPS.
5.2.2. Number of Individuals Required per Task	CA CPS 5.2.2	The policy management and key generation work are designated as two or more personnel to carry out the work as a minimum.

5.3.1. Qualifications, Experience, and Clearance Requirements	CA CPS 5.3.1	Operational personnel must have acquired a nationally recognized information and telecommunications qualification or have a business equivalent to that.
5.3.3. Training Requirements and Procedures	CA CPS 5.3.3	The personnel performing the certification work shall complete the security regulations, internal management procedures and technical education necessary for the performance of the work. Education and training contents are as follows. - Information security (laws, regulations, manuals, etc.) and personal information protection education - Procedures for handling the certification management center and roles, responsibilities, etc. - PKI-based technology and latest certification trend education - Training on identity verification procedures and procedures
5.3.4. Retraining Frequency and Requirements	CA CPS 5.3.4	CA personnel perform security and related technical training annually.
5.3.7. Independent Contractor Controls	CA CPS 5.3.7	No stipulated**.**
5.4.1. Types of Events Recorded	CA CPS 5.4.1	CA system records the following event log. - Event number - Date and time the event occurred - Event Details - Event processing results - Certificate lifecycle-related logs - Certification Authority Key Life Cycle Related Logs

		- The access log and request log for the certification authority(CA) system
5.4.3. Retention Period for Audit Logs	CA CPS 5.4.3	The storage period of the log is kept for 10 years according to the type, considering the availability of the storage space and the efficiency of management.
5.4.8. Vulnerability Assessments	CA CPS 5.4.8	The vulnerability identifies the elements that threaten the functioning of the authentication system and evaluates the technical and administrative elements to reduce the possibility.
5.5.2. Retention Period for Archive	CA CPS 5.5.2	The record keeping period is 10 years.
5.7.1. Incident and Compromise Handling Procedures	CA CPS 5.7.1	In the event of a disaster that poses a serious risk to the operation of the digital signature and authentication system, the infrastructure and computer equipment shall be restored according to the disaster recovery procedure, and the certification work shall be resumed in accordance with the Disaster Recovery Procedure of the Digital Signature Certification Center.
6.1.1. Key Pair Generation	CA CPS 6.1.1	he certificate authority (CA) key pair is generated according to the key generation procedure. Key generation uses HSM with FIPS 140-2 Level 3 certification. Key generation works with at least two authorized personnel. The subscriber's administrative digital signature generation key (private key) pair is generated using the 'certificate management software' provided to the

		subscriber. Key generation uses HSM with FIPS 140-2 Level 3 certification.
6.1.2. Private Key Delivery to Subscriber	CA CPS 6.1.2	Certificate authority private key delivery - N/A Subscriber private key delivery - The software generates a private key on behalf of the subscriber, and passes the private key and certificate to the subscriber.
6.1.5. Key Sizes	CA CPS 6.1.6	RSA: 2048 bit or above
6.1.6. Public Key Parameters Generation and Quality Checking	CA CPS 6.1.6	The certification authority verifies that the public key matches the private key owned by the certification authority. The certification authority verifies the uniqueness of the DN of the subscriber certificate. When issuing new subscriber certificate, confirm the integrity of CMP request using authorization code HMAC.
6.1.7. Key Usage Purposes	CA CPS 6.1.7	The purpose of usage is specified in the X.509 Extension field.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CA CPS 6.2	There is Private Key Protection and Cryptographic Module Engineering Controls on CPS 6.2

6.2.5. Private Key Archival	CA CPS 6.2.5	The certificate authority private key backup equipment should be stored in a separate and safe place.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CA CPS 6.2.6	The certificate authority private key is encrypted and extracted by a hardware security module (HSM) for backup purposes.
6.2.7. Private Key Storage on Cryptographic Module	CA CPS 6.2.7	The certificate authority private key is partitioned inside the hardware security module (HSM) and stored securely.
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	CA CPS 6.3.2	The certification authority certificate (CA) is 10 years and the subscriber certificate is 2 years 3 months.
6.5.1. Specific Computer Security Technical Requirements	CA CPS 6.5.1	CA system has an access control function, an operator identification and verification function, an audit log collection function, and a CRL generation function.
7.1. Certificate profile	CA CPS 7	Digital Signature Certificates, Certificate Revocation List (CRL), and Onsite Certificate Status Protocol (OCSP) complies with "Administrative Digital Signature Technology Requirements".

7.1.1. Version Number(s)	CA CPS 7.1.1	X.509 V3
7.1.2. Certificate Content and Extensions; Application of RFC 5280	CA CPS 7.1.2	The certificate issued by the Certification Center uses the certificate extension field specified in the "Administrative Electronic Signature Technology Requirement".
7.1.2.1 Root CA Certificate	CA CPS 7.1.2	The certificate issued by the Certification Center uses the certificate extension field specified in the "Administrative Electronic Signature Technology Requirement".
7.1.2.2 Subordinate CA Certificate	CA CPS 7.1.2	The certificate issued by the Certification Center uses the certificate extension field specified in the "Administrative Electronic Signature Technology Requirement".
7.1.2.3 Subscriber Certificate	CA CPS 7.1.2	The certificate issued by the Certification Center uses the certificate extension field specified in the "Administrative Electronic Signature Technology Requirement".
7.1.2.4 All Certificates	CA CPS 7.1.2	The certificate issued by the Certification Center uses the certificate extension field specified in the "Administrative Electronic Signature Technology Requirement".

7.1.2.5 Application of RFC 5280	CA CPS 7.1.2	The certificate issued by the Certification Center uses the certificate extension field specified in the "Administrative Electronic Signature Technology Requirement".
7.1.3. Algorithm Object Identifiers	CA CPS 7.1.3	The Certificate Algorithm OID complies with the "Administrative Electronic Signature Technology Requirements" framework.
7.1.4. Name Forms	CA CPS 7.1.4	Issuer DN and subject DN conform to the "Administrative Electronic Signature Technology Requirements" framework.
7.1.4.1 Issuer Information	CA CPS 7.1.4	Issuer DN and subject DN conform to the "Administrative Electronic Signature Technology Requirements" framework.
7.1.4.2 Subject Information	CA CPS 7.1.4	Issuer DN and subject DN conform to the "Administrative Electronic Signature Technology Requirements" framework.
7.1.4.3 Subject Information - Subordinate CA Certificates	CA CPS 7.1.4	Issuer DN and subject DN conform to the "Administrative Electronic Signature Technology Requirements" framework.

7.1.5. Name Constraints	CA CPS 7.1.5	No stipulated**.**
7.1.6. Certificate Policy Object Identifier	CA CPS 7.1.6	The Policy Identifier (OID) of the Certificate Policies conforms to the "Administrative Electronic Signature Technology Requirements" framework.
7.1.6.1 Reserved Certificate Policy Identifiers	CA CPS 7.1.6	The Policy Identifier (OID) of the Certificate Policies conforms to the "Administrative Electronic Signature Technology Requirements" framework.
7.1.6.2 Root CA Certificates	CA CPS 7.1.6	The Policy Identifier (OID) of the Certificate Policies conforms to the "Administrative Electronic Signature Technology Requirements" framework.
7.1.6.3 Subordinate CA Certificates	CA CPS 7.1.6	The Policy Identifier (OID) of the Certificate Policies conforms to the "Administrative Electronic Signature Technology Requirements" framework.
7.1.6.4 Subscriber Certificates	CA CPS 7.1.6	The Policy Identifier (OID) of the Certificate Policies conforms to the "Administrative Electronic Signature Technology Requirements" framework.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	CA CPS 8	All matters of the Administrative Digital Signature Certification Practice Statement comply with domestic and foreign laws and regulations, related technical standards, and carry out periodic audits by independent third parties.
8.1. Frequency or circumstances of assessment	CA CPS 8.1	Audits should be carried out periodically, not to exceed a maximum of one year.
8.2. Identity/qualifications of assessor	CA CPS 8.2	Audits are performed by personnel with certain qualifications and skills as follows. 1. Independent from the auditee 2. Those who have sufficient knowledge of domestic and foreign laws, regulations and related technical standards. 3. PKI technology, information and communication technology and information system audit experts 4. Related international qualifications such as Webtrust, ETSI or equivalent
8.4. Topics covered by assessment	CA CPS 8.4	The scope of the audit includes compliance with the Administrative Digital Signature Certification Practice Statement, certification authority key management, certificate management and Root CA system management.
8.6. Communication of results	CA CPS 8.6	The results of the audit are reported to the Director of the Certification Center.

8.7. Self-Audits	N/A	No stipulated.
9.6.1. CA Representations and Warranties	CA CPS 9.6.1.1	The administrative digital signature certification system shall comply with the relevant laws, regulations, regulations and regulations of Korea. The administrative digital signature authentication system complies with the Administrative Digital Signature Certification Practice Statement (CPS) in relation to the CA business. The administrative digital signature authentication scheme conforms to the relevant standards and rules to provide a secure and reliable authentication system.
9.6.3. Subscriber Representations and Warranties	CA CPS 9.6.3	The user shall provide accurate information for the use of the administrative digital signature authentication service. The certification authority ensures that the certificate user has a reliable signature key algorithm and validation.
9.8. Limitations of liability	CA CPS 9.8	No stipulated.
9.9.1. Indemnification by CAs	CA CPS 9.9.1	No stipulated.

9.16.3. Severability	CA CPS 9.16.3	No stipulated.