PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 11 TAHUN 2024
TENTANG
PENYELENGGARAAN ALGORITMA KRIPTOGRAFI INDONESIA
DAN
PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN NEGARA,

Menimbang : a. bahwa untuk mengamankan dan melindungi informasi elektronik, diperlukan standardisasi keamanan informasi dan penyelenggaraan pengamanan informasi elektronik;

b. bahwa standardisasi keamanan informasi dan penyelenggaraan pengamanan informasi elektronik dapat terwujud melalui penerapan algoritma kriptografi;

c. bahwa untuk memenuhi kebutuhan penilaian kesesuaian dalam melakukan kegiatan penilaian kesesuaian bagi persyaratan acuan standar evaluasi keamanan modul kriptografi serta untuk meningkatkan daya saing Indonesia dan membangun kepercayaan konsumen melalui pemberian jaminan keamanan informasi, perlu menyusun penilaian kesesuaian keamanan modul kriptografi;

d. bahwa ketentuan Pasal 24 Undang-Undang Nomor 20 Tahun 2014 tentang Standardisasi dan Penilaian Kesesuaian serta Pasal 43 Peraturan Pemerintah Nomor 34 Tahun 2018 tentang Sistem Standardisasi dan Penilaian Kesesuaian Nasional mendelegasikan pengaturan skema penilaian kesesuaian terhadap persyaratan acuan ditetapkan oleh kepala lembaga pemerintah nonkementerian yang memberlakukan persyaratan acuan;

e. bahwa Peraturan Kepala Lembaga Sandi Negara Nomor 9 Tahun 2010 tentang Pedoman Sertifikasi Peralatan Sandi dan Peraturan Kepala Lembaga Sandi Negara Nomor 5 Tahun 2014 tentang Standar Algoritma Kriptografi pada Instansi Pemerintah sudah tidak sesuai dengan perkembangan hukum dan kebutuhan organisasi, sehingga perlu diganti;

f. bahwa berdasarkan pertimbangan sebagaimana dimaksud huruf a, huruf b, huruf c, huruf d, dan huruf e, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi;

Mengingat :

1. Undang-Undang Nomor 20 Tahun 2014 tentang Standardisasi dan Penilaian Kesesuaian (Lembaran Negara Republik Indonesia Tahun 214 Nomor 216,. Tambahan Lembaran Negara Republik Indonesia Nomor 5584);
2. Peraturan Pemerintah Nomor 34 Tahun 2018 tentang Sistem Standardisasi dan Penilaian Kesesuaian Nasional (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 110, Tambahan Lembaran Negara Republik Indonesia Nomor 6225);
3. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
4. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803) sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2023 Nomor 544);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG PENYELENGGARAAN ALGORITMA KRIPTOGRAFI INDONESIA DAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. Kriptografi adalah disiplin ilmu yang meliputi prinsip, sarana dan metode untuk menyediakan keamanan informasi, termasuk kerahasiaan, integritas data, autentikasi dan nir-penyangkalan.
2. Algoritma Kriptografi adalah prosedur komputasi yang terdefinisi dengan baik dan memiliki input variabel, termasuk kunci kriptografi dan menghasilkan *output*.
3. Algoritma Kriptografi Indonesia adalah Algoritma Kriptografi yang ditetapkan secara nasional berdasarkan Kriteria Algoritma Kriptografi Indonesia dan digunakan untuk melindungi informasi elektronik pada Sistem Elektronik.
4. Badan Siber dan Sandi Negara yang selanjutnya disebut Badan adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan sandi.
5. Kriteria Algoritma Kriptografi Indonesia adalah ukuran yang menjadi dasar dalam kegiatan pendataan dan penilaian Algoritma Kriptografi yang terdiri dari kriteria umum dan kriteria khusus.
6. Pengusul adalah warga negara Indonesia atau badan hukum pencipta dan/atau pemilik Algoritma Kriptografi yang mengajukan pendaftaran Algoritma Kriptografi.
7. Penyelenggara Sistem Elektronik yang selanjutnya disebut PSE adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/ atau keperluan pihak lain.
8. Pemohon adalah pihak yang mengajukan permohonan sertifikasi Modul Kriptografi serta memiliki kendali penuh terhadap desain dan dokumentasi Modul Kriptografi.
9. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
10. Modul Kriptografi adalah seperangkat perangkat keras, perangkat lunak, dan/atau perangkat tegar yang mengimplementasikan Algoritma Kriptografi dan/atau

fungsi keamanan lain yang dimuat dalam batas kriptografinya.

11. Infrastruktur Informasi Vital yang selanjutnya disebut IIV adalah Sistem Elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional, baik berdiri sendiri maupun saling bergantung dengan Sistem Elektronik lainnya dalam menunjang sektor strategis, yang jika terjadi gangguan, kerusakan, dan/ atau kehancuran pada infrastruktur dimaksud berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional.
12. Deputi adalah pimpinan tinggi madya yang melaksanakan tugas dan fungsi di bidang perumusan kebijakan teknis di bidang strategi dan kebijakan keamanan siber dan sandi di Badan.
13. Direktur adalah pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang koordinasi, perumusan, dan pemantauan kebijakan teknis di bidang teknologi keamanan siber dan sandi di Badan.
14. Skema Penilaian Kesesuaian Keamanan Modul Kriptografi yang selanjutnya disebut Skema PKKMK adalah aturan, prosedur dan/atau manajemen yang berlaku untuk melaksanakan penilaian kesesuaian terhadap keamanan Modul Kriptografi.
15. Standar Nasional Indonesia yang selanjutnya disingkat SNI adalah standar yang ditetapkan oleh Badan Standardisasi Nasional dan berlaku di wilayah Negara Kesatuan Republik Indonesia.
16. Level Keamanan adalah seperangkat persyaratan keamanan yang terdefinisi dengan baik di area keamanan.
17. Sertifikat Keamanan Modul Kriptografi adalah jaminan tertulis yang diberikan LSPro yang menyatakan bahwa Modul Kriptografi teknologi IIV telah memenuhi SNI ISO/IEC 19790:2015.
18. Tanda SNI adalah tanda sertifikasi yang ditetapkan oleh Badan Standardisasi Nasional untuk menyatakan telah terpenuhinya persyaratan acuan SNI.
19. Tanda KMK adalah tanda sertifikasi yang ditetapkan oleh Kepala Badan untuk menyatakan Modul Kriptografi telah memenuhi persyaratan acuan SNI ISO/IEC 19790:2015.
20. Lembaga sertifikasi produk untuk sertifikasi Modul Kriptografi yang merupakan teknologi pelindungan IIV yang selanjutnya disebut LSPro adalah unit kerja di Badan Siber dan Sandi Negara yang melaksanakan tugas dan fungsi di bidang sertifikasi produk keamanan siber dan sandi.

21. Komite Akreditasi Nasional yang selanjutnya disingkat KAN adalah lembaga nonstruktural yang bertugas dan bertanggung jawab di bidang akreditasi lembaga penilaian kesesuaian.

BAB II
PENYELENGGARAAN ALGORITMA KRIPTOGRAFI

Pasal 2

Penyelenggaraan Algoritma Kriptografi Indonesia terdiri atas:
a. penyusunan;
b. reviu;
c. pemanfaatan; dan
d. pengawasan.

Pasal 3

(1) Penyusunan dan reviu sebagaimana dimaksud dalam Pasal 2 huruf a dan huruf b dilaksanakan oleh Badan.
(2) Dalam melaksanakan penyusunan dan reviu sebagaimana dimaksud pada ayat (1), Badan menugaskan komite Algoritma Kriptografi Indonesia.

Pasal 4

Penyusunan Algoritma Kriptografi Indonesia sebagaimana dimaksud dalam Pasal 3 ayat (2) dilakukan dengan mekanisme:
a. adopsi; dan
b. seleksi.

Pasal 5

(1) Adopsi sebagaimana dimaksud dalam Pasal 4 huruf a merupakan kegiatan pendataan dan penilaian Algoritma Kriptografi untuk menjadi kandidat Algoritma Kriptografi Indonesia.
(2) Kegiatan pendataan Algoritma Kriptografi sebagaimana dimaksud pada ayat (1) dilakukan dengan mengumpulkan kandidat Algoritma Kriptografi yang berasal dari standar, publikasi ilmiah bereputasi, dan/atau kompetisi Algoritma Kriptografi berdasarkan kriteria umum Algoritma Kriptografi Indonesia.
(3) Kegiatan penilaian Algoritma Kriptografi sebagaimana dimaksud pada ayat (1) dilakukan melalui pengkajian terhadap hasil kegiatan pendataan Algoritma Kriptografi sebagaimana dimaksud pada ayat (2) berdasarkan kriteria khusus Algoritma Kriptografi Indonesia.
(4) Kriteria khusus sebagaimana dimaksud pada ayat (3) dilaksanakan sesuai dengan jenis Algoritma Kriptografi.

(5) Kriteria umum dan kriteria khusus Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (2) dan ayat (3) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.
(6) Proses adopsi sebagaimana dimaksud pada ayat (1) dilaksanakan dengan jangka waktu minimal 1 (satu) tahun dimulai sejak kegiatan pendataan.

Pasal 6

(1) Seleksi sebagaimana dimaksud dalam Pasal 4 huruf b merupakan proses pendataan dan penilaian Algoritma Kriptografi yang berasal dari pendaftaran Algoritma Kriptografi.
(2) Pendaftaran Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (1) merupakan proses permohonan Algoritma Kriptografi menjadi kandidat Algoritma Kriptografi Indonesia.
(3) Pendaftaran Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (2) disampaikan oleh Pengusul kepada Kepala Badan.
(4) Pengusul sebagaimana dimaksud pada ayat (3) menyampaikan pendaftaran Algoritma Kriptografi Indonesia yang berisi:
    a. informasi Pengusul;
    b. informasi Algoritma Kriptografi; dan
    c. bukti publikasi ilmiah.
(5) Informasi Pengusul sebagaimana dimaksud pada ayat (4) huruf a bagi Pengusul warga negara Indonesia disampaikan dalam bentuk:
    a. salinan kartu tanda penduduk; dan
    b. surat pernyataan kepemilikan Algoritma Kriptografi.
(6) Informasi Pengusul sebagaimana dimaksud pada ayat (4) huruf a bagi Pengusul badan hukum yang berkedudukan di Indonesia disampaikan dalam bentuk:
    a. salinan dokumen legal pendirian badan hukum; dan
    b. surat pernyataan kepemilikan Algoritma Kriptografi.
(7) Informasi Algoritma Kriptografi sebagaimana dimaksud pada ayat (4) huruf b paling sedikit memuat:
    a. nama Algoritma Kriptografi;
    b. jenis Algoritma Kriptografi;
    c. struktur Algoritma Kriptografi dan desain rasional;
    d. kekuatan keamanan;
    e. jenis platform;
    f. implementasi; dan

g. hasil uji yang telah dilakukan.

(8) Bukti publikasi ilmiah sebagaimana dimaksud pada ayat (4) huruf c paling sedikit harus melampirkan surat keterangan publikasi jurnal.

(9) Format surat pendaftaran Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (3) tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

(10) Kegiatan pendataan Algoritma Kriptografi sebagaimana dimaksud pada ayat (1) dilakukan terhadap kandidat Algoritma Kriptografi berdasarkan kriteria umum Algoritma Kriptografi Indonesia.

(11) Kegiatan penilaian Algoritma Kriptografi yang dimaksud pada ayat (1) dilakukan melalui pengkajian dan pengujian terhadap hasil kegiatan pendataan Algoritma Kriptografi sebagaimana dimaksud pada ayat (10) berdasarkan kriteria khusus Algoritma Kriptografi Indonesia.

(12) Kriteria khusus sebagaimana dimaksud pada ayat (11) dilaksanakan sesuai dengan jenis Algoritma Kriptografi.

(13) Kriteria umum dan kriteria khusus Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (10) dan ayat (11) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

(14) Proses seleksi sebagaimana dimaksud pada ayat (1) dilaksanakan dengan jangka waktu minimal 2 (dua) tahun dimulai sejak kegiatan pendataan.

Pasal 7

(1) Kandidat Algoritma Kriptografi Indonesia yang telah melalui mekanisme adopsi dan/atau seleksi sebagaimana dimaksud dalam Pasal 4 direkomendasikan untuk ditetapkan sebagai Algoritma Kriptografi Indonesia.

(2) Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Kepala Badan.

Pasal 8

(1) Reviu sebagaimana dimaksud dalam Pasal 2 huruf b dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

(2) Reviu sebagaimana dimaksud pada ayat (1) dilaksanakan terhadap:
a. kriteria Algoritma Kriptografi Indonesia; dan
b. Algoritma Kriptografi Indonesia.

(3) Reviu terhadap kriteria Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (2) huruf a

dilaksanakan untuk memastikan kriteria Algoritma Kriptografi Indonesia sesuai dengan perkembangan teknologi kriptografi terkini.

(4) Reviu terhadap Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan untuk menjamin kesesuaian Algoritma Kriptografi Indonesia dengan kriteria Algoritma Kriptografi Indonesia.

(5) Hasil reviu kriteria Algoritma Kriptografi Indonesia dan Algoritma Kriptografi Indonesia menjadi rekomendasi dalam pemutakhiran kriteria Algoritma Kriptografi Indonesia dan Algoritma Kriptografi Indonesia.

Pasal 9

(1) Pemanfaatan sebagaimana dimaksud dalam Pasal 2 huruf c dilaksanakan oleh PSE dan Pemohon.

(2) PSE sebagaimana dimaksud pada ayat (1) memanfaatkan Algoritma Kriptografi Indonesia sesuai dengan kategori Sistem Elektronik.

(3) Pemohon sebagaimana dimaksud pada ayat (1) memanfaatkan Algoritma Kriptografi Indonesia untuk diimplementasikan dalam Modul Kriptografi miliknya.

(4) Modul Kriptografi sebagaimana dimaksud pada ayat (3) berupa Modul Kriptografi yang merupakan teknologi pelindungan IIV maupun Modul Kriptografi yang bukan merupakan teknologi pelindungan IIV.

Pasal 10

(1) Pengawasan sebagaimana dimaksud dalam Pasal 2 huruf d dilakukan terhadap kesesuaian Algoritma Kriptografi Indonesia yang diterapkan oleh:
   a. PSE; dan
   b. Pemohon yang menyediakan Modul Kriptografi yang merupakan teknologi pelindungan IIV.

(2) Pengawasan sebagaimana dimaksud pada ayat (1) dilakukan oleh Badan.

(3) Dalam melakukan pengawasan sebagaimana dimaksud pada ayat (2) dapat dilakukan secara mandiri atau bekerja sama dengan instansi terkait berdasarkan penugasan dari Badan.

(4) Hasil Pengawasan sebagaimana yang dimaksud pada ayat (1) dilaporkan kepada Badan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 11

Pengawasan terhadap Pemohon sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf b dilakukan sesuai dengan ketentuan yang terdapat dalam kegiatan penyelenggaraan

penilaian kesesuaian terhadap Modul Kriptografi yang merupakan teknologi pelindungan IIV.

Pasal 12

(1) Komite Algoritma Kriptografi Indonesia sebagaimana dimaksud dalam Pasal 3 ayat (2) ditetapkan dengan keputusan Kepala Badan.
(2) Keputusan Kepala Badan sebagaimana dimaksud pada ayat (1) berlaku selama 3 (tiga) tahun sejak tanggal ditetapkan.
(3) Keanggotaan komite Algoritma Kriptografi Indonesia terdiri atas unsur :
    a. pemerintah;
    b. pakar dan/atau akademisi;
    c. pelaku usaha dan/atau asosiasi pelaku usaha terkait; dan
    d. konsumen dan/atau asosiasi konsumen terkait.
(4) Unsur pemerintah sebagaimana dimaksud pada ayat (3) huruf a merupakan kementerian atau lembaga yang memiliki keterkaitan fungsi di bidang kriptografi, keamanan siber, atau keamanan informasi.
(5) Unsur pakar dan/atau akademisi sebagaimana dimaksud pada ayat (3) huruf b merupakan orang yang memiliki keahlian di bidang kriptografi, keamanan siber, atau keamanan informasi.
(6) Unsur pelaku usaha dan/atau asosiasi pelaku usaha terkait sebagaimana dimaksud pada ayat (3) huruf c merupakan orang, orang yang mewakili badan usaha, atau orang yang mewakili kumpulan pelaku usaha baik berbentuk badan hukum maupun tidak berbentuk badan hukum yang memiliki kepentingan atau menyelenggarakan kegiatan usaha di bidang kriptografi atau keamanan siber atau keamanan informasi.
(7) Unsur konsumen dan/atau asosiasi konsumen terkait sebagaimana dimaksud pada ayat (3) huruf d merupakan orang yang menggunakan produk atau jasa di bidang kriptografi atau keamanan siber atau keamanan informasi.

Pasal 13

(1) Komite Algoritma Kriptografi Indonesia sebagaimana dimaksud dalam Pasal 12 terdiri atas:
    a. pengarah;
    b. ketua merangkap anggota;
    c. sekretaris merangkap anggota; dan
    d. anggota.
(2) Komite Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (1) beranggotakan minimal 9 (sembilan) orang dan maksimal 15 (lima belas) orang.

(3) Komite Algoritma Kriptografi Indonesia sebagaimana dimaksud pada ayat (1) berjumlah ganjil dan satu unsur keanggotaan komite sebagaimana dimaksud pada ayat (1) tidak mendominasi unsur yang lain atau tidak melampaui 50% (lima puluh persen) dari jumlah keseluruhan anggota.

Pasal 14

(1) Pengarah komite Algoritma Kriptografi Indonesia sebagaimana dimaksud dalam Pasal 13 ayat (1) huruf a yaitu Deputi.
(2) Pengarah komite sebagaimana dimaksud pada ayat (1) memiliki tugas untuk memberikan petunjuk dan pengarahan pelaksanaan penyusunan rekomendasi Algoritma Kriptografi Indonesia.

Pasal 15

(1) Ketua komite Algoritma Kriptografi Indonesia sebagaimana dimaksud dalam Pasal 13 ayat (1) huruf b yaitu Direktur.
(2) Ketua komite sebagaimana dimaksud pada ayat (1) memiliki tugas dan tanggung jawab sebagai berikut:
    a. memimpin rapat penyusunan dan reviu terhadap kriteria Algoritma Kriptografi Indonesia dan Algoritma Kriptografi Indonesia;
    b. mengevaluasi kinerja anggota komite Algoritma Kriptografi Indonesia; dan
    c. melaporkan program reviu kriteria Algoritma Kriptografi Indonesia dan Algoritma Kriptografi Indonesia setiap akhir tahun kepada Kepala Badan.

Pasal 16

(1) Sekretaris komite Algoritma Kriptografi Indonesia sebagaimana dimaksud dalam Pasal 13 ayat (1) huruf c merupakan pejabat fungsional ahli madya yang memiliki kompetensi di bidang kriptografi, keamanan siber, atau keamanan informasi pada unit kerja yang melaksanakan tugas dan fungsi di bidang kriptografi pada Badan.
(2) Sekretaris komite sebagaimana dimaksud pada ayat (1) dibantu oleh sekretariat komite Algoritma Kriptografi Indonesia.
(3) Sekretariat komite sebagaimana dimaksud pada ayat (2) bertugas:
    a. membantu ketua komite Algoritma Kriptografi Indonesia dalam melaksanakan tanggung jawabnya;

b. memfasilitasi dan menjamin kelancaran pelaksanaan kegiatan komite Algoritma Kriptografi Indonesia;
c. menyediakan referensi dan sumber daya yang diperlukan untuk kegiatan komite Algoritma Kriptografi Indonesia;
d. memelihara rekaman data dan informasi yang berkaitan dengan kegiatan komite Algoritma Kriptografi Indonesia agar dapat diakses dan ditelusuri secara mudah;
e. menyiapkan evaluasi program kerja dan partisipasi anggota komite Algoritma Kriptografi Indonesia; dan
f. menyiapkan laporan akhir tahun kinerja komite Algoritma Kriptografi Indonesia.

(4) Sekretariat komite sebagaimana dimaksud pada ayat (2) merupakan pejabat atau pegawai pada unit kerja yang melaksanakan tugas dan fungsi di bidang kriptografi.

Pasal 17

(1) Anggota komite Algoritma Kriptografi Indonesia sebagaimana dimaksud dalam Pasal 13 ayat (1) huruf d harus memiliki kriteria sebagai berikut:
a. memiliki penguasaan dan/atau pengalaman minimal 2 (dua) tahun di bidang kriptografi, keamanan siber, keamanan informasi, dan/atau bidang lain yang relevan; dan
b. memiliki komitmen untuk melaksanakan tugas sebagai anggota komite Algoritma Kriptografi Indonesia yang dibuktikan dengan surat pernyataan sebagaimana tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

(2) Anggota komite sebagaimana dimaksud pada ayat (1) bertugas:
a. melakukan kegiatan pendataan dan penilaian Algoritma Kriptografi berdasarkan kriteria umum yang berasal dari:
1. standar, publikasi ilmiah bereputasi, dan/atau kompetisi Algoritma Kriptografi; dan
2. Algoritma Kriptografi yang berasal dari pendaftaran Algoritma Kriptografi.
b. melakukan pengkajian terhadap hasil kegiatan pendataan Algoritma Kriptografi yang berasal dari standar, publikasi ilmiah bereputasi dan/atau kompetisi Algoritma Kriptografi berdasarkan kriteria khusus Algoritma Kriptografi Indonesia;
c. melakukan pengkajian dan pengujian terhadap Algoritma Kriptografi yang berasal dari

pendaftaran Algoritma Kriptografi, berdasarkan kriteria khusus Algoritma Kriptografi Indonesia;

d. memberikan rekomendasi kandidat Algoritma Kriptografi Indonesia yang telah melalui tahap penilaian dan tahap pengkajian untuk ditetapkan sebagai Algoritma Kriptografi Indonesia;
e. melaksanakan reviu paling sedikit 1 (satu) kali dalam 1 (satu) tahun terhadap:
   1. kriteria Algoritma Kriptografi Indonesia; dan
   2. Algoritma Kriptografi Indonesia; dan
f. memberikan rekomendasi hasil reviu dalam rangka pemutakhiran kriteria Algoritma Kriptografi Indonesia dan Algoritma Kriptografi Indonesia.

BAB III
PENYELENGGARAAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI

Pasal 18

Penyelenggaraan penilaian kesesuaian sebagaimana dimaksud dalam Pasal 11 terdiri atas komponen:

a. Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV; dan
b. penyelenggara Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV.

Pasal 19

Skema PKKMK sebagaimana dimaksud dalam Pasal 18 huruf a menggunakan persyaratan acuan SNI ISO/IEC 19790:2015 teknologi informasi - teknik keamanan - persyaratan keamanan untuk modul kriptografi.

Pasal 20

(1) Persyaratan acuan sebagaimana dimaksud dalam Pasal 19 diberlakukan secara wajib bagi Pemohon yang menyediakan Modul Kriptografi yang merupakan teknologi pelindungan IIV.
(2) Modul Kriptografi sebagaimana dimaksud pada ayat (1) minimal memenuhi Level Keamanan 2 (dua).

Pasal 21

(1) Skema PKKMK sebagaimana dimaksud dalam Pasal 18 huruf a terdiri atas:
   a. ruang lingkup;
   b. persyaratan acuan;
   c. jenis kegiatan penilaian kesesuaian;
   d. prosedur administratif;
   e. determinasi;

f. tinjauan dan keputusan;
g. pemeliharaan sertifikasi;
h. evaluasi khusus;
i. ketentuan pengurangan lingkup sertifikasi, pembekuan dan pencabutan sertifikat;
j. keluhan dan banding;
k. informasi publik;
l. daftar Modul Kriptografi, acuan SNI dan uraian penilaian kesesuaian; dan
m. kriteria kompetensi personel atau tim dalam kegiatan sertifikasi.

(2) Rincian Skema PKKMK sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 22

(1) Kewajiban pemenuhan persyaratan acuan sebagaimana dimaksud dalam Pasal 20 dibuktikan dengan:
a. kepemilikan Sertifikat Keamanan Modul Kriptografi yang dikeluarkan oleh LSPro yang diselenggarakan Badan; dan
b. surat persetujuan penggunaan Tanda SNI dan Tanda KMK yang dikeluarkan oleh Badan.

(2) Penggunaan Tanda SNI dan Tanda KMK dapat dilakukan setelah Pemohon mendapatkan surat persetujuan sebagaimana dimaksud pada ayat (1) huruf b.

(3) Ketentuan penggunaan Tanda SNI dan Tanda KMK sebagaimana dimaksud pada ayat (2) tercantum dalam Lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 23

(1) Penyelenggara Skema PKKMK sebagaimana dimaksud dalam Pasal 18 huruf b terdiri atas:
a. pemilik Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV;
b. komite Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV;
c. LSPro; dan
d. laboratorium pengujian untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV.

(2) Penyelenggara Skema PKKMK sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 24

(1) LSPro untuk sertifikasi Modul Kriptografi yang merupakan teknologi pelindungan IIV ditunjuk oleh Kepala Badan.
(2) Penunjukan LSPro oleh Kepala Badan dalam bentuk surat keputusan.
(3) LSPro sebagaimana dimaksud pada ayat (1) melakukan:
    a. penerbitan Sertifikat Keamanan Modul Kriptografi bagi teknologi pelindungan IIV sesuai dengan persyaratan acuan;
    b. pelaporan Sertifikat Keamanan Modul Kriptografi yang telah diterbitkan dan/atau dicabut kepada Kepala Badan melalui Deputi paling lambat 7 (tujuh) hari kerja sejak tanggal penerbitan atau pencabutan; dan
    c. pelaporan surveilans secara berkala dan/atau tidak terjadwal, berdasarkan pengaduan kepada Kepala Badan melalui Deputi, paling lambat 7 (tujuh) hari kerja sejak tanggal penetapan laporan surveilans.
(4) LSPro sebagaimana dimaksud pada ayat (1) wajib terakreditasi oleh KAN.
(5) Dalam hal LSPro belum terakreditasi oleh KAN sebagaimana dimaksud pada ayat (4), harus memenuhi kewajiban akreditasi paling lama 2 (dua) tahun sejak tanggal penunjukan.

Pasal 25

(1) Laboratorium pengujian untuk sertifikasi Modul Kriptografi yang merupakan teknologi pelindungan IIV ditunjuk oleh Kepala Badan.
(2) Penunjukan laboratorium pengujian sebagaimana dimaksud pada ayat (1) dilakukan terhadap laboratorium pengujian yang telah terakreditasi oleh KAN untuk lingkup yang sesuai.
(3) Dalam hal laboratorium pengujian sebagaimana dimaksud pada ayat (2) belum tersedia atau jumlahnya belum mencukupi kebutuhan, Kepala Badan dapat menunjuk laboratorium pengujian yang sudah diakreditasi oleh KAN untuk ruang lingkup yang sejenis.

Pasal 26

(1) Penunjukan laboratorium pengujian sebagaimana dimaksud dalam Pasal 25 ayat (3), dilakukan berdasarkan hasil evaluasi dalam rangka penunjukan laboratorium pengujian oleh Deputi.
(2) Evaluasi dalam rangka penunjukan laboratorium pengujian sebagaimana dimaksud pada ayat (1) mencakup:

a. aspek legalitas kelembagaan; dan
b. kemampuan untuk melakukan pengujian Modul Kriptografi yang relevan dengan persyaratan yang ditetapkan dalam SNI, berdasarkan pertimbangan:
   1. sarana pengujian dan metode uji yang digunakan untuk pengujian Modul Kriptografi; dan
   2. personel laboratorium pengujian dalam jumlah yang memadai untuk pengujian Modul Kriptografi.

(3) Laboratorium pengujian yang ditunjuk Kepala Badan sebagaimana dimaksud pada ayat (1) wajib diakreditasi oleh KAN sesuai dengan lingkup produk yang disertifikasi paling lama 2 (dua) tahun terhitung sejak tanggal penunjukan.

Pasal 27

LSPro dan laboratorium pengujian yang ditunjuk oleh Kepala Badan sebagaimana dimaksud dalam Pasal 24 sampai dengan Pasal 26 diawasi oleh Kepala Badan melalui Deputi.

Pasal 28

Tata cara penunjukan dan pengawasan LSPro dan/atau laboratorium pengujian sebagaimana dimaksud dalam Pasal 24 sampai dengan Pasal 27 tercantum dalam Lampiran VI yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 29

(1) Pengawasan pemenuhan persyaratan acuan sebagaimana dimaksud dalam Pasal 20 dilakukan oleh Badan melalui Deputi.
(2) Pengawasan sebagaimana dimaksud pada ayat (1) dilaksanakan secara berkala dan/atau secara khusus terhadap Modul Kriptografi yang termasuk teknologi pelindungan IIV.
(3) Pengawasan secara berkala sebagaimana dimaksud pada ayat (2) dilakukan minimal 1 (satu) kali dalam 24 (dua puluh empat) bulan setelah pengawasan sebelumnya.
(4) Pengawasan secara khusus sebagaimana dimaksud pada ayat (2) dilakukan jika terdapat pengaduan.
(5) Dalam melakukan pengawasan sebagaimana dimaksud pada ayat (1), Badan dapat berkoordinasi dengan kementerian, lembaga pemerintah non kementerian, dan/atau pemerintah daerah.
(6) Pengawasan sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:

a. pemeriksaan proses produksi; dan
b. pemeriksaan mutu,

melalui pengambilan sampel di lokasi produksi dan/atau di luar lokasi produksi yang dilakukan secara acak.

(7) Sampel sebagaimana dimaksud pada ayat (6) diuji oleh laboratorium pengujian yang telah ditunjuk oleh Kepala Badan.

(8) Hasil pengawasan sebagaimana dimaksud pada ayat (1) dilaporkan oleh Deputi kepada Kepala Badan.

Pasal 30

(1) Pelanggaran ketentuan persyaratan acuan sebagaimana dimaksud dalam Pasal 20 oleh Pemohon yang telah mendapatkan Sertifikat Keamanan Modul Kriptografi serta Tanda SNI dan Tanda KMK dikenai sanksi berupa:
a. pembekuan Sertifikat Keamanan Modul Kriptografi;
b. pencabutan Sertifikat Keamanan Modul Kriptografi;
c. pencabutan surat persetujuan penggunaan Tanda SNI dan Tanda KMK;
d. menghentikan kegiatan perdagangan Modul Kriptografi yang merupakan teknologi pelindungan IIV; atau
e. menarik Modul Kriptografi yang merupakan teknologi pelindungan IIV dari peredaran.

(2) Pembekuan atau pencabutan sertifikat sebagaimana dimaksud pada ayat (1) huruf a dan huruf b, dilakukan oleh LSPro berdasarkan rekomendasi Kepala Badan

(3) Pencabutan surat persetujuan sebagaimana dimaksud pada ayat (1) huruf c dilakukan oleh Kepala Badan.

(4) Penghentian perdagangan dan penarikan Modul Kriptografi sebagaimana dimaksud pada ayat (1) huruf d dan huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB IV
REKOGNISI

Pasal 31

(1) Pemohon yang memiliki hasil pengujian keamanan Modul Kriptografi yang merupakan teknologi pelindungan IIV yang diterbitkan oleh laboratorium pengujian negara lain yang telah terakreditasi untuk lingkup yang sesuai wajib mengajukan permohonan rekognisi kepada Badan.

(2) Rekognisi sebagaimana dimaksud pada ayat (1) dapat dilakukan jika:
   a. badan Akreditasi telah menandatangani perjanjian saling pengakuan (*mutual recognition arrangement*) melalui kerja sama akreditasi internasional;
   b. negara memiliki perjanjian bilateral di bidang regulasi teknis dengan pemerintah Republik Indonesia; atau
   c. negara memiliki perjanjian multilateral di bidang regulasi teknis dengan pemerintah Republik Indonesia.

(3) Badan melakukan rekognisi sebagaimana dimaksud pada ayat (1) sesuai dengan ketentuan peraturan perundangan-undangan.

BAB V
KETENTUAN PERALIHAN

Pasal 32

Pada saat Peraturan Badan ini mulai berlaku:
a. permohonan sertifikasi yang sedang diproses tetap dilaksanakan berdasarkan skema yang diacu dalam Peraturan Kepala Lembaga Sandi Negara Nomor 9 Tahun 2010 tentang Pedoman Sertifikasi Peralatan Sandi; dan
b. Sertifikat Keamanan Modul Kriptografi yang telah diterbitkan oleh LSPro, tetap berlaku sampai dengan berakhirnya jangka waktu sertifikat.

BAB VI
KETENTUAN PENUTUP

Pasal 33

Pada saat Peraturan Badan ini mulai berlaku, Peraturan Kepala Lembaga Sandi Negara nomor 9 tahun 2010 tentang Pedoman Sertifikasi Peralatan Sandi (Berita Negara Republik Indonesia Tahun 2010 Nomor 185) dan Peraturan Kepala Lembaga Sandi Negara nomor 5 tahun 2014 tentang Standar Algoritma Kriptografi pada Instansi Pemerintah (Berita Negara Republik Indonesia Tahun 2014 Nomor 1862), dicabut dan dinyatakan tidak berlaku.

Pasal 34

Peraturan Badan ini mulai berlaku 6 (enam) bulan terhitung sejak tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Badan ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 19 November 2024

KEPALA BADAN SIBER DAN SANDI NEGARA,

Ditandatangani secara elektronik oleh:
KEPALA BADAN SIBER DAN SANDI NEGARA

Hinsa Siburian
Letnan Jenderal TNI (Purn)

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 20 November 2024

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM REPUBLIK INDONESIA,

#KUMHAMPASTI

Ditandatangani secara elektronik oleh :

DHAHANA PUTRA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2024 NOMOR 853

LAMPIRAN I
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 11 TAHUN 2024
TENTANG
PENYELENGGARAAN ALGORITMA KRIPTOGRAFI INDONESIA DAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI

KRITERIA UMUM DAN KRITERIA KHUSUS ALGORITMA KRIPTOGRAFI INDONESIA

A. KRITERIA UMUM ALGORITMA KRIPTOGRAFI

Kriteria umum Algoritma Kriptografi Indonesia terdiri atas:

1. Persyaratan lisensi
   Algoritma Kriptografi Indonesia harus bebas royalti.
2. Domain publik: Algoritma Kriptografi harus dipublikasikan untuk jangka waktu minimal 3 (tiga) tahun terakhir di domain publik yaitu:
   a. konferensi, lokakarya dan simposium asosiasi internasional untuk penelitian kriptografis (*international association for cryptologic research*) yaitu:
      1) *asiacrypt*, *crypto, eurocrypt*;
      2) *international workshop on fast software encryption*;
      3) *international workshop on cryptographic hardware and embedded systems*;
      4) *conference on practice and theory in public key cryptography*;
      5) *theory of cryptography conference*;
      6) *real world crypto symposium*; atau
   b. konferensi, lokakarya dan simposium bekerja sama dengan asosiasi internasional untuk penelitian kriptografis (*international association for cryptologic research*) yaitu:
      1) *international conference on post-quantum cryptography;*
      2) *international conference on cryptography*;
      3) *code-based cryptography workshop*;
      4) *current trends in cryptology workshop*;
      5) *financial cryptography and data security*;
      6) *selected areas in cryptography*;
      7) *conference on security and cryptography for networks;*
      8) *international conference on cryptology in india*;
      9) *conference on security standards research*;
      10) *international workshop on lightweight cryptography for security and privacy*;
      11) *workshop on fault diagnosis and tolerance in cryptography*; atau
   c. konferensi tahunan *institute of electrical and electronics engineers*:
      1) *symposium on security and privacy*;

2) *symposium on the foundations of computer science*; atau

d. konferensi tahunan *association for computing machinery*:
   1) *symposium on theory of computing*;
   2) *computer and communication security*; atau

e. konferensi internasional ternama yang memiliki sejarah lebih dari 15 (lima belas) tahun serta memiliki ketersediaan prosiding:
   1) *usenix security*;
   2) *european symposium on research in computer security*;
   3) *australasian conference on information security and privacy*;
   4) *international conference on information security and cryptography*; atau

f. jurnal ternama ┼minimum dikutip oleh *database systems and logic programming*:
   1) *association for computing machinery*:
      a) *journal of the association for computing machinery*;
      b) *communications of the association for computing machinery*; atau
   2) elsevier:
      a) *computer communications*;
      b) *information and computation*;
      c) *journal of computer and system sciences*;
      d) *journal of discrete algorithms*; atau.
   3) *institute of electrical and electronics engineers*:
      a) *institute of electrical and electronics engineers transactions on information theory*;
      b) *institute of electrical and electronics engineers transactions on computers*;
      c) *institute of electrical and electronics engineers security and privacy*; atau
   4) *institute of electronics, information and communication engineers*:
      a) *institute of electronics, information and communication engineers transactions on fundamentals of electronics, communications and computer sciences*;
      b) *institute of electronics, information and communication engineers transactions on information and systems*; atau
   5) *society for industrial and applied mathematics*: *society for industrial and applied mathematics journal on computing*; atau
   6) springer:
      a) *combinatorica*;
      b) *cryptography and communications*;
      c) *designs, codes and cryptography*;
      d) *journal of cryptology*;
      e) *international journal of information security*; atau

7) *international association for cryptologic research*: *transactions on symmetric cryptography*; atau

g. standar lainnya: publikasi resmi sebagai standar dalam bahasa Inggris, atau terjemahan yang disetujui oleh organisasi standardisasi yang diakui dan telah tersedia untuk umum (hanya berlaku untuk mekanisme adopsi); atau

h. kompetisi nasional dan internasional untuk memilih Algoritma Kriptografi yang terbuka untuk umum dan telah dijalankan selama minimal 2 (dua) tahun, serta memenuhi analisis dan publikasi konferensi, lokakarya, jurnal, simposium atau standar lainnya.

3. Adopsi industri: Algoritma Kriptografi telah terimplementasi pada aplikasi komersial yang menggunakan sistem kriptografi baik secara nasional atau secara internasional.

B. KRITERIA KHUSUS ALGORITMA KRIPTOGRAFI

Kriteria	Algoritma Kriptografi pada sistem elektronik rendah	Algoritma Kriptografi pada sistem elektronik tinggi	Algoritma Kriptografi pada sistem elektronik strategis
Algoritma Simetrik			
Sandi Blok (*Block Cipher*)			
Panjang kunci	minimal 128 (seratus dua puluh delapan) bit	minimal 192 (seratus sembilan puluh dua) bit	minimal 256 (dua ratus lima puluh enam) bit
Ukuran blok	minimal 128 (seratus dua puluh delapan) bit		
Lulus uji keacakan	• lulus 15 (lima belas) uji statistik yang terdapat dalam dokumen SP 800-22 Revisi 1a (setiap uji menggunakan 9 (sembilan) tipe data). Kesembilan tipe data tersebut adalah *key avalanche, plaintext avalanche, plaintext/ciphertext correlation, cipher block chaining mode, random plaintext/random keys, low density plaintext, low density keys, high density plaintext,* dan *high density keys*. • batas lulus uji keacakan yang dapat diterima yaitu apabila jumlah maksimum sampel yang ditolak (s) tidak lebih dari hasil perhitungan interval konfidensi (IK) dengan tingkat kepercayaan sebesar $\alpha = 0{,}01$ dengan rumus: $s < \lfloor IK \rfloor$ dengan $IK = \left[n\left(\alpha + 3\sqrt{\frac{\alpha(1-\alpha)}{n}} \right) \right]$ dan $n =$ ukuran sampel		

Kriteria	Algoritma Kriptografi pada sistem elektronik rendah	Algoritma Kriptografi pada sistem elektronik tinggi	Algoritma Kriptografi pada sistem elektronik strategis
Ketahanan terhadap serangan	• kriptanalisis linear (*linear cryptanalysis*) • kriptanalisis diferensial *(differential cryptanalysis)* dengan kompleksitas komputasi serangan kriptanalisis tersebut tidak lebih besar dari serangan *brute force* yang dirumuskan dengan: $C << \min(2^k, 2^n)$ dimana $C = \max(C_d, C_p, C_s)$ dengan: k : panjang kunci, n : panjang blok, C_d: kompleksitas data (*data complexity*), C_p: kompleksitas waktu (*time complexity*)/ kompleksitas pemrosesasn (*processing complexity*), C_s: kompleksitas memori (*memory complexity*)/kompleksitas penyimpanan (*storage complexity*)		
Sandi Alir (*Stream Cipher*)			
Panjang kunci	minimal 128 (seratus dua puluh delapan) bit		
Lulus uji keacakan	lulus 15 (lima belas) uji statistik yang terdapat dalam dokumen SP 800-22 Revisi 1a		
Ketahanan terhadap serangan	• serangan aljabar (*algebraic attack)* • serangan korelasi (*correlation attack)* • serangan *distinguishing* (*distinguishing attack)* • serangan *guess-and-determine* (*guess-and-determine attack*)		
Pembangkit Bit Acak Deterministik (*Deterministic Random Bit Generators*) berdasarkan skema Pembangkit Bit Acak Deterministik pada ISO/IEC 18031			
1. Pembangkit Bit Acak Deterministik berbasis Fungsi *Hash* (*Deterministic Random Bit Generators Based On Hash Function*)			
a. Pembangkit Bit Acak Deterministik *Hash* (*Hash Deterministic Random Bit Generators*)			
Kekuatan keamanan (*Security Strength)*	128 (seratus dua puluh delapan) bit	192 (seratus sembilan puluh dua) bit	256 (dua ratus lima puluh enam) bit

Kriteria	Algoritma Kriptografi pada sistem elektronik rendah	Algoritma Kriptografi pada sistem elektronik tinggi	Algoritma Kriptografi pada sistem elektronik strategis
Minimum Entropy	128 (seratus dua puluh delapan) bit	192 (seratus sembilan puluh dua) bit	256 (dua ratus lima puluh enam) bit
Panjang *seed (seedlen)*	440 (empat ratus empat puluh) bit		
Lulus uji keacakan	lulus 15 (lima belas) uji statistik yang terdapat dalam dokumen SP 800-22 Revisi 1a		
Ketahanan terhadap serangan	• *forward secrecy* • *backward secrecy* • tidak dapat diprediksi (*unpredictable*)		
b. Pembangkit Bit Acak Deterministik Kode Autentikasi Pesan *Hash* (*Hash Message Authentication Code Deterministic Random Bit Generators*)			
Kekuatan keamanan (*Security Strength)*	128 (seratus dua puluh delapan) bit	192 (seratus sembilan puluh dua) bit	256 (dua ratus lima puluh enam) bit
Minimum Entropy	128 (seratus dua puluh delapan) bit	192 (seratus sembilan puluh dua) bit	256 (dua ratus lima puluh enam) bit
Panjang *seed (seedlen)*	440 (empat ratus empat puluh) bit		888 (delapan ratus delapan puluh delapan) bit
Lulus uji keacakan	lulus 15 (lima belas) uji statistik yang terdapat dalam dokumen SP 800-22 Revisi 1a		
Ketahanan terhadap serangan	• *forward secrecy* • *backward secrecy* • tidak dapat diprediksi (*unpredictable*)		
2. Pembangkit Bit Acak Deterministik Berbasis Sandi Blok (*Deterministic Random Bit Generators Based On Block Cipher*)			
Kekuatan keamanan (*Security Strength)*	128 (seratus dua puluh delapan) bit	192 (seratus sembilan puluh dua) bit	256 (dua ratus lima puluh enam) bit

Kriteria	Algoritma Kriptografi pada sistem elektronik rendah	Algoritma Kriptografi pada sistem elektronik tinggi	Algoritma Kriptografi pada sistem elektronik strategis
Minimum entropy	128 (seratus dua puluh delapan) bit	192 (seratus sembilan puluh dua) bit	256 (dua ratus lima puluh enam) bit
Panjang *Seed*	256 (dua ratus lima puluh enam) bit	320 (tiga ratus dua puluh) bit	384 (tiga ratus delapan puluh empat) bit
Panjang blok Input dan *Output* (*blocklen*)	128 (seratus dua puluh delapan) bit		
Panjang *Counter field* (*ctr_len*)	4 (empat) s.d. 128 (seratus dua puluh delapan)		
Max number of bits per request (untuk $B = (2^{ctr\_len} - 4) \times 128$)	$\min(B, 2^{19})$		
Reseed interval	2^{48}		
Lulus uji keacakan	lulus 15 (lima belas) uji statistik yang terdapat dalam dokumen SP 800-22 Revisi 1a		
Ketahanan terhadap serangan	• *forward secrecy* • *prediction resistance* • tidak dapat diprediksi (*unpredictable*)		
Fungsi *Hash* (*Hash function*)			
Ukuran *digest*	256 (dua ratus lima puluh enam) bit		
Panjang pesan maksimum (*Maximum message length*)	$2^{64}-1$		

Kriteria	Algoritma Kriptografi pada sistem elektronik rendah	Algoritma Kriptografi pada sistem elektronik tinggi	Algoritma Kriptografi pada sistem elektronik strategis
Ketahanan terhadap serangan	• ketahanan *Pre-image* (*Pre-image resistance)* • ketahanan *Second pre-image* (*Second pre-image resistance*) • ketahanan kolisi (*Collision resistance*)		
Algoritma Asimetrik			
A. Primitif (berdasarkan FIPS PUB 186-4)			
1. Problem faktorisasi integer (*Integer factorization problem*)	Ukuran modulus (k) minimal 3072 (tiga ribu tujuh puluh dua) bit		
2. Problem logaritma diskrit (*Discrete Logarithm Problem*)	• Panjang L minimal 3072 (tiga ribu tujuh puluh dua) bit dimana L adalah panjang modulus bilangan prima p dengan $2^{L-1} < p < 2^L$ • Panjang N minimal 256 (dua ratus lima puluh enam) bit dengan N adalah panjang dari q dimana q merupakan pembagi bilangan prima (*prime divisor*) dari $(p-1)$ dengan $2^{N-1} < q < 2^N$		
3. Problem logaritma diskrit kurva eliptis/EC DLP (*Elliptic Curve Discrete Logarithm Problem based Algorithm*)	Ukuran n minimal 256 (dua ratus lima puluh enam) bit dengan n adalah orde titik G dimana G merupakan titik basis orde prima pada kurva (*base point of prime order on the curve*)		
Kekuatan keamanan (*Security Strength)*	minimal 128 (seratus dua puluh delapan) bit		

Kriteria	Algoritma Kriptografi pada sistem elektronik rendah	Algoritma Kriptografi pada sistem elektronik tinggi	Algoritma Kriptografi pada sistem elektronik strategis
Ketahanan terhadap serangan	keamanan teks sandi terpilih adaptif (*adaptive chosen ciphertext security)*		
B. Skema			
1. Skema enkripsi asimetrik (*Asymmetric encryption scheme*)			
Kekuatan keamanan (*Security Strength*	minimal 128 (seratus dua puluh delapan) bit		
Ukuran kunci	sesuai dengan kriteria ukuran kunci algoritma primitif yang digunakan		
Ketahanan terhadap serangan	• tahan terhadap serangan teks sandi terpilih adaptif (*adaptive chosen ciphertext attack*) • terbukti aman dalam model *oracle* acak *(provably secure in the random oracle model)*		
2. Skema tanda tangan digital asimetrik (*Asymmetric digital signature scheme*)			
Kekuatan keamanan (*Security Strength*	minimal 128 (seratus dua puluh delapan) bit		
Ukuran kunci	sesuai dengan kriteria ukuran kunci algoritma primitif yang digunakan		
Ketahanan terhadap serangan	Terbukti aman dalam model *oracle* acak *(provably secure in the random oracle model*)		

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

LAMPIRAN II
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 11 TAHUN 2024
TENTANG
PENYELENGGARAAN ALGORITMA KRIPTOGRAFI INDONESIA DAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI

FORMAT SURAT PENDAFTARAN ALGORITMA KRIPTOGRAFI INDONESIA DAN SURAT PERNYATAAN KOMITMEN ANGGOTA KOMITE ALGORITMA KRIPTOGRAFI INDONESIA

A. Format surat pendaftaran Algoritma Kriptografi Indonesia
   1. Surat Permohonan Pendaftaran

[Nama badan hukum Pengusul]
[Alamat badan hukum Pengusul]
[Nomor Telepon Dan Surel badan hukum Pengusul]

Kepada Yth.

Kepala Badan Siber dan Sandi Negara
di
Jakarta

[Nama Pengusul] dengan ini mengajukan permohonan pendaftaran Algoritma Kriptografi. Bersama ini kami sampaikan pula kelengkapan dokumen dalam bentuk *hardcopy* dan/atau *softcopy*[*)] sebagai berikut:

1 Informasi Pengusul
2 Informasi Produk Algoritma Kriptografi
3 Bukti Publikasi Ilmiah
4 Penyataan Bebas Royalti

Demikian permohonan ini, kelengkapan dokumen dan/atau data yang dipersyaratkan dan dilampirkan, kami bertanggung jawab atas kebenaran dari dokumen dan/atau data dimaksud. Atas dukungannya, kami ucapkan terima kasih.

[Jabatan Pengusul]

.....
[Nama Pengusul]

[*)]Coret yang tidak perlu

1. INFORMASI PENGUSUL
Tanggal:
Asal pengusul: ☐ Warga Negara Indonesia (WNI) ☐ Badan Hukum (Sebutkan):
Identitas Pengusul:
Nama:
Alamat:
Kota:
Provinsi:
Negara:
Kode Pos:
Nomor Telepon/fax
Nomor Hp
Email:
Tanda Tangan Pengusul

2. INFORMASI ALGORITMA KRIPTOGRAFI	
Nama Algoritma Kriptografi	
Deskripsi Singkat Algoritma Kriptografi:	
Jenis Algoritma Kriptografi	☐ Sandi blok (*block cipher*) ☐ Sandi alir (*stream cipher*) ☐ Pembangkit bilangan acak Deterministik (*Deterministic Random Number Generators*) ☐ Pembangkit bilangan acak deterministik berbasis fungsi *hash* (*Deterministic Random Number Generators Based on Hash Function*) ☐ Pembangkit bilangan acak deterministik berbasis sandi blok (*Deterministic Random Number Generators Based on Block Cipher*) ☐ Fungsi *hash* (*Hash function*) ☐ Algoritma asimetrik (*Asymmetric algorithm*) ☐ Primitif ☐ Skema enkripsi asimetrik (*Asymmetric encryption scheme*)

2. INFORMASI ALGORITMA KRIPTOGRAFI	
	☐ Skema tanda tangan digital asimetrik (*Asymmetric digital signature scheme*)
Kekuatan keamanan (*security strength*) yang diusulkan	☐ 128 bit ☐ 192 bit ☐ 256 bit ☐ lain-lain, sebukan Click or tap here to enter text.
Jenis Platform	☐ Perangkat keras ☐ Perangkat lunak ☐ Perangkat tegar ☐ Perangkat lunak-hibrida (*Software-hybrid*) ☐ Perangkat tegar -hibrida (*Firmware-hybrid*)
Implementasi	Sebutkan*) Click or tap here to enter text. *) sebagai contoh: *Bluetooth,* GSM, RFID, kartu cerdas
Hasil uji yang telah dilakukan/ laporan analisis	☐ Sandi Blok (*Block cipher*) ☐ Kriptanalisis linear (*Linear cryptanalysis*) ☐ Kriptanalisis diferensial (*Differential cryptanalysis*) ☐ 15 (lima belas) uji statistik yang terdapat dalam dokumen SP 800-22 Revisi 1a (setiap uji menggunakan 9 (sembilan) tipe data) ☐ Uji vektor (*Test vectors*) Uji vektor yang harus disediakan dengan ketentuan sebagai berikut: • jumlah kunci*:* minimal sebanyak 3 (tiga) buah kunci untuk setiap ukuran kunci; • jumlah pasangan teks terang dan teks sandi minimal sebanya 3 (tiga) buah untuk setiap ukuran kunci; • teks terang dan teks sandi harus diproses dengan menggunakan mode operasi ECB (*Electronic Code Book*) dengan menggunakan *pading* berupa bit 0 (nol)

2. INFORMASI ALGORITMA KRIPTOGRAFI	
	• memberikan hasil keluaran dari setiap *rouncd* ☐ Lain-lain, sebutkan Click or tap here to enter text. ☐ Sandi alir (*stream cipher*) ☐ Serangan aljabar (*algebraic attack*) ☐ Serangan korelasi (*correlation attack*) ☐ Serangan *distinguishing* (*distinguishing attack*) ☐ Serangan *guess-and-determine* (*guess-and-determine attack*) ☐ 15 (lima belas) uji statistik yang terdapat dalam dokumen SP 800-22 Revisi 1a ☐ Uji vektor (*Test vectors*) Uji vektor yang harus disediakan dengan ketentuan sebagai berikut: • jumlah kunci*:* minimal sebanyak 3 (tiga) buah kunci untuk setiap ukuran kunci; • jumlah vektor inisialisasi (*initialization*): minimal sebanyak 3 (tiga) buah kunci untuk setiap ukuran kunci; • ukuran rangkaian kunci yang dibangkitkan sepanjang 256 bit. ☐ Lain-lain, sebutkan Click or tap here to enter text. ☐ Pembangkit bilangan acak deterministik (*Deterministic Random Number Generators*) ☐ Pembangkit bilangan acak deterministik berbasis fungsi *hash* (*Deterministic Random Number Generators Based on Hash Function*) ☐ Pembangkit bilangan acak deterministik berbasis sandi blok (*Deterministic Random Number Generators Based on Block Cipher*) ☐ *Forward secrecy*

2. INFORMASI ALGORITMA KRIPTOGRAFI	
	☐ *Backward secrecy* ☐ Tidak dapat diprediksi (*unpreditable*) ☐ 15 (lima belas) uji statistik yang terdapat dalam dokumen SP 800-22 Revisi 1a ☐ Lain-lain, sebutkan Click or tap here to enter text. ☐ Fungsi *hash* (*Hash function*) ☐ Ketahanan *pre-image* (*Pre-image resistance*) ☐ Ketahanan *second pre-image* (*Second pre-image resistance*) ☐ Ketahanan kolisi (*Collision resistance*) ☐ Uji vektor (*Test vectors*) Uji vektor yang harus disediakan dengan ketentuan sebagai berikut: • jumlah sampel untuk setiap ukuran data minimal 3 sampel; • memberikan hasil keluaran dari setiap *round* ☐ Lain-lain, sebutkan Click or tap here to enter text. ☐ Algoritma asimetrik ☐ Permaslahan matematika yang sulit dan asumsi-asumsinya (*hard mathematical problems and assumptions*) ☐ Model keamanan dan pembuktiannya (*security model and it's proof*) ☐ Uji vektor (*Test vectors*) Uji vektor yang harus disediakan dengan ketentuan sebagai berikut: • jumlah pasangan kunci*:* minimal sebanyak 3 (tiga) buah pasangan kunci; • jumlah sampel yang diproses untuk setiap ukuran kunci: minimal 2 (dua) sampel ☐ Lain-lain, sebutkan

3. BUKTI PUBLIKASI ILMIAH	
Jenis Publikasi (dapat memilih lebih dari 1 (satu))	☐ konferensi, lokakarya dan simposium *international association for cryptologic research* ☐ *asiacrypt* dan/atau *crypto* dan/atau *eurocrypt* ☐ *international workshop on fast software encryption*; ☐ *international workshop on cryptographic hardware and embedded systems*; ☐ *conference on practice and theory in public key cryptography*; ☐ *theory of cryptography conference*; ☐ *real world crypto symposium* ☐ konferensi, lokakarya dan simposium bekerja sama dengan *international association for cryptologic research* ☐ *international conference on post-quantum cryptography;* ☐ *international conference on cryptography*; ☐ *code-based cryptography workshop*; ☐ *current trends in cryptology workshop*; ☐ *financial cryptography and data security*; ☐ *selected areas in cryptography;* ☐ *conference on security and cryptography for networks;* ☐ *international conference on cryptology in india*; ☐ *conference on security standards research*; ☐ *international workshop on lightweight cryptography for security and privacy;* atau ☐ *workshop on fault diagnosis and tolerance in cryptography*; ☐ konferensi tahunan *institute of electrical and electronics engineers* ☐ *symposium on security and privacy*; ☐ *symposium on the foundations of computer science*; ☐ konferensi tahunan *association for computing machinery* ☐ *symposium on theory of computing*; ☐ *computer and communication security* ☐ konferensi internasional ternama yang memiliki sejarah lebih dari 15 (lima belas) tahun serta memiliki ketersediaan prosiding

3. BUKTI PUBLIKASI ILMIAH	
	☐ USENIX *security*; ☐ *european symposium on research in computer security*; ☐ *australasian conference on information security and privacy*; atau ☐ *international conference on information security and cryptography*; ☐ jurnal ternama minimum dikutip oleh *database system and logic programming* ☐ *association for computing machinery* ☐ *journal of the association for computing machinery*; atau ☐ *communications of the association for computing machinery* ☐ elsevier ☐ *computer communications*; ☐ *information and computation*; ☐ *journal of computer and system sciences*; atau ☐ *journal of discrete algorithms* ☐ *institute of electrical and electronics engineers* ☐ *institute of electrical and electronics engineers transactions on information theory*; ☐ *institute of electrical and electronics engineers transactions on computers*; atau ☐ *institute of electrical and electronics engineers security and privacy* ☐ *institute of electronics, information and communication engineers* ☐ *institute of electronics, information and communication engineers transactions on fundamentals of electronics, communications and computer sciences*; atau ☐ *institute of electronics, information and communication engineers transactions on information and systems* ☐ *springer* ☐ *combinatorica*; ☐ *cryptography and communications*; ☐ *designs, codes and cryptography*; ☐ *journal of cryptology*; atau

3. BUKTI PUBLIKASI ILMIAH	
	☐ *international journal of information security* ☐ *society for industrial and applied* ☐ *international association for cryptologic research*: *transactions on symmetric cryptography mathematics*: *society for industrial and applied mathematics journal on computing* ☐ Kompetisi untuk memilih Algoritma Kriptografi yang terbuka untuk umum dan kompetisi tersebut telah dijalankan selama minimal 2 (dua) tahun ☐ tingkat nasional, sebutkan ☐ tingkat internasional, sebutkan

4. KELENGKAPAN PERSYARATAN DOKUMEN
☐ Surat Pernyataan Kepemilikan Algoritma ☐ Salinan Identitas Pengusul (KTP) ☐ Salinan Dokumen Legal Pendirian Badan Hukum Indonesia ☐ Dokumen tentang Informasi Algoritma Kriptografi yang Diusulkan ☐ Dokumen Desain Rasional dari Algoritma Kriptografi yang Diusulkan ☐ Surat Keterangan Publikasi Ilmiah ☐ Hasil Uji Algoritma yang telah dilakukan ☐ *Intellectual Property statements/ agreements / disclosures* ☐ Kelengkapan lain, sebutkan

5. KONTAK UNTUK PENYAMPAIAN HASIL			
Nama Penanggung Jawab:			
Email :	Nomor Telp :	Nomor HP:	Fax:

6. PERNYATAAN PERSETUJUAN
▪ Kami menyatakan bahwa informasi yang diisi di dalam formulir ini adalah benar dan tepat. ▪ Kami bersedia menerima syarat dan ketentuan seleksi Algoritma Kriptografi Indonesia

Tempat, tanggal
Jabatan Pemohon

Nama Pemohon

2. Pernyataan Bebas Royalti

[Nama badan hukum Pengusul]
[Alamat badan hukum Pengusul]
[Nomor Telepon Dan Surel badan hukum Pengusul]

Saya yang bertanda tangan di bawah ini:

1	Nama	:	[Nama]
2	Alamat Badan Hukum (Sesuai dengan Surat Keterangan Domisili)	:	[Tulis alamat lengkap] [Nama Gedung, Lantai] [Nama Jalan diikuti Nomor Kavling
3	Nama Algoritma Kriptografi	:	[Nama Algoritma Kriptografi]

menyatakan bebas royalti untuk penggunaan komersial dan non-komersial dari [Nama Algoritma Kriptografi] dalam aplikasi yang tidak tertanam (*non-embedded applications*) dan aplikasi tertanam (*embedded applications*). Selain pembatasan hukum yang berlaku pada algoritma enkripsi (jika ada), lisensi ini akan diterbitkan berdasarkan non-diskriminatif.

Demikian pernyataan ini saya buat dengan sebenarnya.

Tempat, tanggal
[Jabatan Pemohon]

Tanda tangan
dan
materai 10000

[Nama Pemohon]

B. Surat pernyataan komitmen anggota Komite Algoritma Kriptografi Indonesia

SURAT PERNYATAAN
KOMITE ANGGOTA KRIPTOGRAFI INDONESIA

Saya yang bertanda tangan di bawah ini:

Nama	:
Instansi	:
Alamat	:
Email	:
Nomor Telepon	:
Nomor Fax	:

dengan ini menyatakan akan berpartisipasi dalam kegiatan Komite Algoritma Kriptografi Indonesia selaku : Ketua/Sekretaris/Anggota*).

Tempat, tanggal

Tanda tangan

(Nama Jelas)

*) Coret yang tidak perlu

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

LAMPIRAN III
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 11 TAHUN 2024
TENTANG
PENYELENGGARAAN ALGORITMA KRIPTOGRAFI INDONESIA DAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI

RINCIAN SKEMA PKKMK UNTUK MODUL KRIPTOGRAFI YANG MERUPAKAN TEKNOLOGI PELINDUNGAN IIV

A. Ruang Lingkup

Dokumen ini berlaku untuk acuan pelaksanaan Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV berdasarkan persyaratan acuan SNI ISO/IEC 19790:2015 yang tercantum dalam tabel daftar Modul Kriptografi, acuan SNI dan uraian penilaian kesesuaian.

B. Persyaratan Acuan

Persyaratan acuan Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV mencakup:

1. SNI ISO/IEC 19790:2015 sebagaimana tercantum pada tabel daftar Modul Kriptografi, acuan SNI dan uraian penilaian kesesuaian;
2. SNI dan standar lain yang diacu dalam SNI sebagaimana dimaksud pada tabel daftar Modul Kriptografi, acuan SNI dan uraian penilaian kesesuaian; dan/atau
3. Peraturan lain yang diterbitkan oleh Badan.

C. Jenis Kegiatan Penilaian Kesesuaian

Penilaian kesesuaian dilakukan dengan kegiatan sertifikasi oleh LSPro yang ditetapkan oleh Kepala Badan dan telah diakreditasi oleh KAN berdasarkan SNI ISO/IEC 17065 untuk lingkup Modul Kriptografi sesuai tabel daftar Modul Kriptografi, acuan SNI dan uraian penilaian kesesuaian. Kegiatan sertifikasi yang dilakukan oleh LSPro terdiri atas sertifikasi Modul Kriptografi.

D. Prosedur Administratif

1. Pengajuan Permohonan Sertifikasi
   a. LSPro harus menyusun format permohonan sertifikasi bagi Pemohon untuk mendapatkan seluruh informasi.
   b. Pengajuan permohonan sertifikasi dilakukan oleh Pemohon dan akan dicatat serta diverifikasi oleh LSPro. Kriteria Pemohon yang dapat mengajukan sertifikasi sesuai dengan ketentuan peraturan perundang-undangan.
   c. Permohonan sertifikasi harus dilengkapi dengan:
      1) informasi Pemohon:
         a) nama dan alamat Pemohon, serta nama dan kedudukan atau jabatan personel yang bertanggung jawab atas pengajuan permohonan sertifikasi;

b) bukti pemenuhan persyaratan izin berusaha sesuai dengan ketentuan peraturan perundang-undangan;
c) merek Modul Kriptografi yang diajukan untuk disertifikasi (telah terdaftar atau sedang didaftarkan di Direktorat Jenderal Kekayaan Intelektual Kementerian Hukum dan HAM RI;
d) apabila Pemohon melakukan pembuatan Modul Kriptografi dengan merek yang dimiliki oleh pihak lain, menyertakan bukti perjanjian yang mengikat secara hukum untuk melakukan pembuatan Modul Kriptografi untuk pihak lain;
e) apabila Pemohon bertindak sebagai pemilik merek yang mengalihdayakan proses produksinya kepada pihak lain, menyertakan bukti kepemilikan merek dan perjanjian alih daya pelaksanaan produksi dengan pihak lain;
f) apabila Pemohon bertindak sebagai perwakilan resmi pemilik merek yang berkedudukan hukum di luar negeri, menyertakan bukti perjanjian yang mengikat secara hukum tentang penunjukan sebagai perwakilan resmi pemilik merek di wilayah Republik Indonesia; dan
g) pernyataan bahwa Pemohon bertanggung jawab penuh atas pemenuhan persyaratan acuan SNI ISO/IEC 19790:2015 dan pemenuhan persyaratan proses sertifikasi, serta bersedia memberikan akses terhadap lokasi dan/atau informasi yang diperlukan oleh LSPro dalam melaksanakan kegiatan sertifikasi.

2) informasi Modul Kriptografi:
a) informasi merek Modul Kriptografi yang diajukan untuk disertifikasi;
b) SNI yang digunakan sebagai dasar pengajuan permohonan sertifikasi sesuai tabel daftar Modul Kriptografi, acuan SNI dan uraian penilaian kesesuaian;
c) formulir pengajuan permohonan sertifikasi Modul Kriptografi
d) dokumen dan informasi terkait Modul Kriptografi yang meliputi:
(1) laporan hasil uji Algoritma Kriptografi dari laboratorium pengujian yang ditunjuk oleh Kepala Badan;
(2) dokumen desain Modul Kriptografi;
(3) dokumen kebijakan keamanan (*security policy*) sebagaimana dipersyaratkan SNI ISO/IEC 19790 (termasuk tipe, versi dan Level Keamanan Modul Kriptografi);
(4) dokumen model *finite state*, berupa model matematis dari proses sekuensial mesin yang terdiri dari input, keluaran, kondisi, fungsi yang memetakan kondisi input ke *output*, transisi kondisi, dan spesifikasi yang menggambarkan kondisi awal;

(5) dokumen panduan penggunaan dan konfigurasi Modul Kriptografi;
(6) Modul Kriptografi (khusus untuk Modul Kriptografi berbentuk perangkat lunak); dan
(7) kode sumber Modul Kriptografi.

3) informasi proses produksi pembuatan Modul Kriptografi:
a) nama, alamat, dan legalitas hukum pembuat Modul Kriptografi apabila berbeda dengan legalitas pemohon);
b) struktur organisasi; nama dan jabatan personel penanggung jawab proses produksi;
c) informasi tentang proses pembuatan Modul Kriptografi yang diajukan untuk disertifikasi, termasuk proses yang dialihdayakan ke pihak lain;
d) informasi terdokumentasi terkait pengelolaan proses produksi yang dipersyaratkan dalam SNI sesuai tabel daftar Modul Kriptografi, Acuan SNI dan Uraian Penilaian kesesuaian;
e) lokasi produksi dan/atau lokasi gudang penyimpanan Modul Kriptografi di wilayah Republik Indonesia; dan
f) apabila telah tersedia, menyertakan sertifikat penerapan sistem manajemen mutu berdasarkan SNI ISO 9001 atau SNI ISO/IEC 27001 dari lembaga sertifikasi yang diakreditasi oleh KAN atau badan akreditasi penandatangan *international accreditaion forum/asia pasific accreditation cooperation multilateral recognition agreement* dengan ruang lingkup yang sesuai atau sistem manajemen lainnya yang relevan.

2. Seleksi
a. Tinjauan permohonan sertifikasi
1) LSPro harus memastikan bahwa informasi yang diperoleh dari permohonan Sertifikasi yang diajukan oleh Pemohon telah lengkap dan memenuhi persyaratan, serta dapat memastikan kemampuan LSPro untuk menindaklanjuti permohonan sertifikasi.
2) Tinjauan permohonan sertifikasi harus dilakukan oleh personel yang memiliki kompetensi sesuai kriteria kompetensi personel atau tim dalam kegiatan sertifikasi.

b. Penandatanganan perjanjian sertifikasi
Setelah permohonan sertifikasi dinyatakan lengkap dan memenuhi persyaratan serta Pemohon menyetujui persyaratan dan prosedur sertifikasi yang ditetapkan oleh lembaga sertifikasi, dilakukan pemutakhiran register Modul Kriptografi Indonesia dan penandatanganan perjanjian sertifikasi oleh Pemohon dan LSPro.

c. Penyusunan rencana evaluasi
1) Berdasarkan informasi yang diperoleh dari persyaratan permohonan sertifikasi yang disampaikan oleh Pemohon, LSPro menetapkan rencana evaluasi yang mencakup paling sedikit:

a) jadwal kegiatan evaluasi yang terdiri atas tujuan, durasi, lokasi, tim, metode pengujian dan agenda evaluasi Modul Kriptografi yang diajukan untuk disertifikasi;
b) rencana pengambilan sampel yang meliputi merek dan tipe Modul Kriptografi yang diajukan untuk disertifikasi dan metode pengambilan sampel sesuai dengan persyaratan acuan SNI ISO/IEC 19790:2015, yang diperlukan untuk pengujian Modul Kriptografi dan mewakili Modul Kriptografi yang diajukan untuk disertifikasi; dan
c) waktu yang diperlukan untuk pelaksanaan pengujian berdasarkan persyaratan acuan metode uji yang dipersyaratkan;

2) Pelaksanaan evaluasi dilakukan oleh auditor atau tim audit yang memiliki kriteria kompetensi sesuai kriteria kompetensi personel/tim dalam kegiatan sertifikasi.
3) Apabila relevan, tahap seleksi juga mengacu pada hal-hal spesifik sebagaimana diatur pada tabel daftar Modul Kriptografi, acuan SNI dan uraian penilaian kesesuaian.

E. Determinasi

Determinasi mencakup 2 (dua) tahap, yaitu evaluasi tahap 1 (satu) dan evaluasi tahap 2 (dua).

1. Pelaksanaan evaluasi tahap 1 (satu)
   a. Evaluasi tahap 1 (satu) dilakukan terhadap kesesuaian informasi Modul Kriptografi dan proses produksi yang disampaikan Pemohon terhadap terhadap lingkup Modul Kriptografi yang ditetapkan persyaratan acuan SNI ISO/IEC 19790:2015 dan peraturan terkait untuk menentukan kesiapan penilaian audit proses produksi.
   b. Apabila hasil evaluasi tahap 1 (satu) menunjukan ketidaksesuaian informasi Modul Kriptografi dan proses produksi, Pemohon diberikan kesempatan untuk melakukan tindakan perbaikan dalam jangka waktu paling lama 5 (lima) hari kerja sejak pemberitahuan kekurangan kelengkapan informasi Modul Kriptografi dan proses produksi diterima oleh Pemohon.
   c. Dalam hal Pemohon tidak dapat menyelesaikan tindakan perbaikan terhadap ketidaksesuaian evaluasi tahap 1 (satu) sesuai jangka waktu yang ditetapkan, LSPro dapat menghentikan proses sertifikasi dan tidak melanjutkan proses sertifikasi ke tahap berikutnya.
2. Pelaksanaan evaluasi tahap 2 (dua)
   a. Evaluasi tahap 2 (dua) dilaksanakan melalui audit proses produksi pembuatan Modul Kriptografi dan pengujian terhadap sampel Modul Kriptografi berdasarkan persyaratan acuan SNI ISO/IEC 19790:2015.
   b. Pengambilan sampel Modul Kriptografi dilakukan oleh personel kompeten yang ditugaskan LSPro. Pengambilan sampel dilakukan di lokasi produksi dengan jumlah sampel sebagaimana

diuraikan pada daftar Modul Kriptografi, acuan SNI, dan uraian penilaian kesesuaian.

c. Audit proses produksi bertujuan untuk memastikan kemampuan dan konsistensi Pemohon dalam memproduksi Modul Kriptografi sesuai dengan persyaratan acuan SNI ISO/IEC 19790:2015 dan sistem manajemen jika relevan.
d. Audit proses produksi dilakukan pada saat Pemohon melakukan proses produksi pembuatan Modul Kriptografi yang diajukan untuk disertifikasi.
e. Audit dilakukan dengan metode audit yang merupakan kombinasi dari audit dokumen dan rekaman, wawancara, observasi, demonstrasi, atau metode audit lainnya.
f. Audit dilakukan terhadap:
    1) tanggung jawab dan komitmen manajemen puncak terhadap konsistensi mutu Modul Kriptografi;
    2) ketersediaan dan pengendalian informasi prosedur dan rekaman pengendalian mutu;
    3) pengelolaan sumber daya termasuk personel, bangunan dan fasilitas, serta lingkungan kerja yang memengaruhi mutu Modul Kriptografi;
    4) tahapan kritis proses produksi Modul Kriptografi, mulai dari bahan baku sampai Modul Kriptografi jadi paling sedikit sebagaimana diuraikan pada tahapan kritis proses produksi Modul Kriptografi pada tabel daftar Modul Kriptografi, acuan SNI dan uraian penilaian kesesuaian;
    5) kelengkapan serta fungsi peralatan produksi termasuk peralatan pengendalian mutu;
    6) bukti verifikasi berdasarkan hasil kalibrasi atau hasil verifikasi peralatan produksi yang membuktikan bahwa peralatan tersebut memenuhi persyaratan produksi. Hasil verifikasi peralatan produksi dapat ditunjukan dengan prosedur yang diperlukan untuk mencapai kondisi atau persyaratan yang ditetapkan; dan
    7) pengendalian proses produksi dan penanganan Modul Kriptografi yang tidak sesuai.
g. Apabila Pemohon telah menerapkan dan mendapatkan sertifikat sistem manajemen mutu berdasarkan SNI ISO 9001 atau SNI ISO/IEC 27001 dari LSPro yang diakreditasi oleh KAN atau badan akreditasi penandatangan *international accreditaion forum*/a*sia pasific accreditation cooperation multilateral recognition agreement* dengan ruang lingkup yang sesuai, maka audit proses produksi dilakukan terhadap implementasi sistem manajemen terkait mutu produk dan huf f f angka 4) sampai dengan angka 7).
h. Apabila hasil audit proses produksi ditemukan ketidaksesuaian pada pengendalian proses dan mutu Modul Kriptografi yang berakibat pada kegagalan Modul Kriptografi dalam memenuhi persyaratan acuan SNI ISO/IEC 19790:2015, maka LSPro memberikan kesempatan kepada Pemohon agar dapat dilakukan

tindakan perbaikan dalam jangka waktu tertentu sesuai dengan kebijakan LSPro.

i. Pengujian Modul Kriptografi dilakukan di laboratorium pengujian yang telah ditunjuk oleh Kepala Badan dan telah dilakukan akreditasi oleh KAN.
j. Pengujian Modul Kriptografi dilakukan terhadap 11 (sebelas) area keamanan sebagaimana dipersyaratkan pada SNI ISO/IEC 19790:2015.
k. Dalam melaksanakan pengujian Modul Kriptografi, laboratorium pengujian menyusun:
   1) Kertas kerja Modul Kriptografi untuk masing-masing area keamanan; dan
   2) Laporan pengujian Modul Kriptografi.
l. Laboratorium pengujian menyampaikan kertas kerja Modul Kriptografi dan Laporan pengujian Modul Kriptografi kepada LSPro untuk mendapatkan reviu dan persetujuan.
m. Pelaksanaan pengujian Modul Kriptografi diawasi auditor LSPro melalui:
   1) rapat kemajuan evaluasi untuk mereviu dan menyetujui kertas kerja Modul Kriptografi untuk masing-masing area Keamanan; dan
   2) melakukan reviu Laporan pengujian Modul Kriptografi.
n. Dalam hal ditemukan ketidaksesuaian pada proses evaluasi tahap 2 (dua), Pemohon dapat diberi kesempatan untuk melakukan tindakan perbaikan dalam jangka waktu tertentu sesuai dengan kesepakatan antara LSPro, laboratorium pengujian dan Pemohon dengan melakukan pemutakhiran pada proposal proyek evaluasi (*evaluation project proposal*).
o. Dalam hal Pemohon tidak dapat menyelesaikan tindakan perbaikan terhadap ketidaksesuaian evaluasi tahap 2 (dua) sesuai jangka waktu yang ditetapkan, LSPro dapat menghentikan proses sertifikasi dan menetapkan bahwa Modul Kriptografi tidak lulus sertifikasi.

F. Tinjauan dan keputusan

1. Tinjauan
   a. Tinjauan hasil evaluasi dilakukan terhadap pemenuhan seluruh persyaratan sertifikasi dan kesesuaian proses sertifikasi, mulai dari pengajuan permohonan sertifikasi, pelaksanaan seleksi dan determinasi serta tindakan perbaikan dari Pemohon jika ada.
   b. Tinjauan hasil evaluasi dinyatakan dalam bentuk rekomendasi tertulis tentang pemenuhan persyaratan acuan SNI ISO/IEC 19790:2015 yang diajukan oleh Pemohon untuk Modul Kriptografi yang diajukan untuk disertifikasi.
   c. Tinjauan hasil evaluasi harus dilakukan oleh orang atau sekelompok orang yang tidak terlibat dalam proses penilaian.
   d. Personel yang melakukan tinjauan hasil penilaian harus memiliki kompetensi sesuai kriteria kompetensi personel atau tim dalam kegiatan sertifikasi.

2. Penetapan keputusan Sertifikasi
   a. Penetapan keputusan sertifikasi dilakukan berdasarkan rekomendasi yang dihasilkan dari proses tinjauan.
   b. Penetapan keputusan sertifikasi harus dilakukan oleh satu orang atau sekelompok orang yang tidak terlibat dalam proses evaluasi.
   c. Penetapan keputusan sertifikasi dapat dilakukan oleh satu orang atau sekelompok orang yang sama dengan yang melakukan tinjauan.
   d. Penetapan keputusan sertifikasi dilakukan oleh personel yang memiliki kompetensi sesuai kriteria kompetensi personel atau tim dalam kegiatan sertifikasi.
   e. Rekomendasi untuk keputusan sertifikasi berdasarkan hasil tinjauan harus didokumentasikan.
   f. LSPro harus memberitahukan secara tertulis kepada Pemohon terkait keputusan sertifikasi.
   g. LSPro harus memberitahu secara tertulis kepada Pemohon terkait alasan menunda atau tidak memberikan keputusan sertifikasi, dan harus mengidentifikasi alasan keputusan tersebut.
   h. Apabila Pemohon menunjukan keinginan untuk melanjutkan proses sertifikasi setelah LSPro memutuskan tidak lulus sertifikasi, Pemohon dapat mengajukan kembali permohonan sertifikasi.
   i. Setelah melakukan penetapan keputusan sertifikasi, LSPro melakukan pemutakhiran register Modul Kriptografi Indonesia dengan status telah disertifikasi.
3 Bukti Kesesuaian
   a. Bukti kesesuaian berupa Sertifikat Keamanan Modul Kriptografi yang diterbitkan oleh LSPro. LSPro menerbitkan Sertifikat Keamanan Modul Kriptografi kepada Pemohon yang telah memenuhi persyaratan acuan SNI ISO/IEC 19790:2015. Sertifikat Keamanan Modul Kriptografi berlaku selama 5 (lima) tahun setelah diterbitkan.
   b. Sertifikat Keamanan Modul Kriptografi terhadap persyaratan acuan SNI ISO/IEC 19790:2015 paling sedikit harus memuat:
      1) nomor sertifikat atau identifikasi penomoran unik lainnya;
      2) nama dan alamat lembaga sertifikasi;
      3) nama dan alamat Pemohon (pemegang sertifikat);
      4) nomor atau identifikasi lain yang mengacu ke perjanjian sertifikasi;
      5) tujuan penggunaan Modul Kriptografi untuk digunakan di sektor IIV;
      6) pernyataan kesesuaian yang mencakup:
         a) merek, versi, tipe dan spesifikasi dari Modul Kriptografi yang dinyatakan memenuhi persyaratan;
         b) Level Keamanan untuk Modul Kriptografi;
         c) persyaratan acuan SNI ISO/IEC 19790:2015 yang menjadi dasar sertifikasi; dan

d) nama dan alamat lokasi produksi pembuatan Modul Kriptografi yang dinyatakan memenuhi persyaratan sesuai lingkup SNI.
7) status akreditasi atau pengakuan LSPro;
8) tanggal penerbitan sertifikat dan masa berlakunya, serta riwayat sertifikat; dan
9) tanda tangan yang mengikat secara hukum dari personel yang bertindak atas nama LSPro sesuai dengan ketentuan peraturan perundang-undangan.

c. Sertifikat dapat dinyatakan tidak berlaku apabila:
1) penyalahgunaan Sertifikat Keamanan Modul Kriptografi oleh Pemohon;
2) penyalahgunaan nama dan logo Badan, LSPro, Tanda SNI dan Tanda KMK oleh Pemohon; atau
3) konflik kepentingan yang mengakibatkan keberpihakan dalam proses sertifikasi.

G. Pemeliharaan Sertifikasi

1. Pengawasan oleh LSPro
a. Pengawasan oleh LSPro dilakukan dengan kegiatan surveilans. Jarak antara surveilans paling sedikit 18 (delapan belas) bulan.
b. LSPro harus melaksanakan kunjungan surveilans paling sedikit 2 (dua) kali dalam periode sertifikasi. Surveilans pertama dilaksanakan pada bulan ke 20 (dua puluh) sampai dengan 24 (dua puluh empat), surveilans kedua dilaksanakan pada bulan ke 40 (empat puluh) sampai dengan 44 (empat puluh empat). Kunjungan surveilans dilakukan melalui kegiatan audit proses produksi dan/atau pengujian Modul Kriptografi.
c. Surveilans dapat dilakukan dengan audit dokumen/rekaman dan/atau melalui audit jarak jauh dengan menggunakan media yang disepakati untuk mendapatkan bukti objektif.
d. Pelaksanaan surveilans juga mengacu pada hal-hal spesifik sebagaimana diatur pada tabel daftar Modul Kriptografi, acuan SNI dan uraian penilaian kesesuaian.

2. Sertifikasi ulang
a. Sertifikasi ulang terhadap Modul Kriptografi dapat dilakukan berdasarkan kondisi masa berlaku Sertifikat Keamanan Modul Kriptografi pada Modul Kriptografi telah berakhir.
b. Apabila proses sertifikasi ulang belum selesai sampai masa berlaku sertifikat berakhir, maka:
1) apabila keterlambatan sertifikasi disebabkan oleh LSPro, maka LSPro menerbitkan surat keterangan yang menyatakan Pemohon sedang dalam proses sertifikasi;
2) apabila keterlambatan sertifikasi disebabkan oleh Pemohon, maka proses sertifikasi tidak dilanjutkan dan sertifikat tidak berlaku.
c. LSPro harus menyampaikan informasi kepada Pemohon untuk melaksanakan sertifikasi ulang Modul Kriptografi paling lambat 9 (sembilan) bulan sebelum masa berlaku sertifikat berakhir.

d. Pelaksanaan sertifikasi ulang dilakukan sesuai dengan tahapan pada prosedur administratif, determinasi, serta tinjauan dan keputusan.
e. Apabila berdasarkan hasil sertifikasi ulang ditemukan ketidaksesuaian, Pemohon harus diberi kesempatan untuk melakukan tindakan perbaikan dalam jangka waktu tertentu sesuai dengan kebijakan LSPro.
f. Sertifikasi ulang dapat dilakukan dengan audit dokumen/rekaman dan/atau melalui audit jarak jauh dengan menggunakan media yang disepakati untuk mendapatkan bukti objektif.

H. Evaluasi Khusus
1. LSPro dapat melaksanakan evaluasi khusus dalam rangka audit perluasan lingkup maupun tindak lanjut atau investigasi atas keluhan atau informasi yang ada.
2. Tahapan evaluasi khusus dalam rangka perluasan lingkup dilakukan sesuai dengan tahapan prosedur administratif namun terbatas pada perluasan lingkup yang diajukan. Evaluasi terhadap perluasan lingkup sertifikasi dapat dilakukan terpisah maupun bersamaan dengan surveilans.
3. Evaluasi khusus dalam rangka investigasi keluhan atau informasi yang ada dilakukan oleh auditor yang memiliki kompetensi untuk melakukan investigasi dan terbatas pada permasalahan yang ada, serta dilakukan dalam waktu yang singkat dari diperolehnya keluhan atau informasi.
4. Berdasarkan hasil evaluasi khusus, apabila terdapat Modul Kriptografi yang disertifikasi tidak memenuhi persyaratan yang ditetapkan, maka LSPro mewajibkan Pemohon untuk menarik semua Modul Kriptografi yang terindikasi tidak sesuai, melaporkan kepada Badan dan melarang mencantumkan Tanda SNI dan Tanda KMK pada Modul Kriptografi dan/atau media lain sejak tanggal terjadinya ketidaksesuaian tersebut sampai dengan dapat dilakukan tindakan perbaikan. Tanda SNI dan Tanda KMK dapat dicantumkan kembali setelah dilakukan tindakan perbaikan dan dinyatakan memenuhi oleh lembaga sertifikasi.

I. Ketentuan Pengurangan Lingkup Sertifikasi, Pembekuan Dan Pencabutan Sertifikat
1. Pengurangan lingkup sertifikasi
Pemohon dapat mengajukan pengurangan lingkup sertifikasi selama periode sertifikasi.
2. Pembekuan dan pencabutan sertifikat
a. LSPro dapat membekukan sertifikat apabila Pemohon:
1) tidak menyetujui untuk dilaksanakan surveilans dan/atau evaluasi khusus;
2) tidak mampu memperbaiki ketidaksesuaian yang diterbitkan oleh LSPro pada saat surveilans dan/atau saat evaluasi khusus; atau

3) menyampaikan permintaan pembekuan sertifikat kepada LSPro.

b. LSPro harus membatasi periode pembekuan sertifikat maksimal 6 (enam) bulan.

c. LSPro dapat melakukan pencabutan sertifikat apabila pemohon:
   1) tidak menyetujui untuk dilaksanakan surveilans dan/atau evaluasi khusus melebihi batas waktu yang ditentukan;
   2) tidak mampu memperbaiki ketidaksesuaian yang mengakibatkan pembekuan sertifikat melebihi batas waktu yang ditentukan; atau
   3) menyampaikan permintaan pencabutan sertifikat kepada LSPro.

d. LSPro dapat mempertimbangkan pembekuan atau pencabutan sertifikat, atau tindakan lainnya yang disebabkan oleh faktor lainnya dengan mempertimbangkan risiko yang ditemukan.

J. Keluhan dan Banding

LSPro harus mengembangkan aturan penanganan keluhan dan banding dengan mempertimbangkan kompetensi dan imparsialitas pelaksanaan penanganan keluhan dan banding.

K. Informasi Publik

LSPro harus mempublikasikan informasi kepada publik sesuai persyaratan SNI ISO/IEC 17065 termasuk informasi Pemohon yang disertifikasi, dibekukan dan dicabut. Informasi publik terkait informasi Pemohon yang disertifikasi, dibekukan dan dicabut tersebut juga harus disampaikan melalui sistem informasi LSPro.

L. Daftar Modul Kriptografi, Acuan SNI dan Uraian Penilaian kesesuaian

No.	Nama Modul Kriptografi	SNI, Judul SNI	Seleksi	Determinasi	Surveilan	Titik Kritis
1	Modul Kriptografi yang merupakan teknologi pelindungan IIV dengan kategori: a. Sistem dan peranti kontrol akses (*Access control devices and system*); b. *Boundary protection devices and system*; c. Pelindungan data (*Data protection*); d. Basis data (*Database*); e. Sistem dan peranti deteksi (*Detection devices and system*); f. Sirkuit terpadu, kartu pintar dan sistem dan peranti terkait kartu pintar (*ICs, smart card and smart card related devices and system*); g. Sistem manajemen kunci (*Key management system*); h. Mobilitas (*Mobility*); i. Piranti multi-fungsi (*Multi-function devices*); j. Jaringan dan sistem dan piranti	SNI ISO/IEC 19790:2015 teknologi informasi - teknik keamanan - persyaratan keamanan untuk modul kriptografi	1) Klasifikasi Modul Kriptografi berdasarkan kategori Modul Kriptografi dan minimal memenuhi Level Keamanan 2 (dua) 2) Khusus untuk perangkat lunak, Pemohon menyerahkan Modul Kriptografi kepada LSPro	1) Pengambilan sampel 3 (tiga) buah untuk sertifikasi awal yang dilakukan oleh Pemohon yang dibuktikan dengan Berita Acara Pengambilan Sampel. 2) Penerapan Sistem Manajemen Mutu atau yang relevan	Pengambilan sampel Modul Kriptografi berbentuk perangkat keras sebanyak 1 (satu) buah untuk sertifikasi ulang dan/ atau sesuai dengan kebutuhan pengujian atau persyaratan acuan SNI ISO/IEC 19790:2015	1) Bahan baku/komponen (tidak berlaku untuk Modul Kriptografi berupa perangkat lunak) Komponen lain sesuai dengan spesifikasi yang ditentukan dan telah memenuhi aspek keselamatan dibuktikan dengan sertifikat komponen. Apabila bahan baku/komponen termasuk kategori SNI Wajib maka dilakukan pemeriksaan Tanda SNI . 2) Penyiapan desain a) Dilakukan dengan menentukan persyaratan keamanan dan pilihan fitur keamanan yang tepat yang dapat memitigasi potensi ancaman dan kerentanan keamanan yang diidentifikasi. b) Dilakukan dengan menggunakan prinsip dan arsitektur desain keamanan untuk mempertimbangkan potensi risiko. Tahap ini melibatkan pemodelan ancaman, kontrol akses, mekanisme kriptografi dan menggunakan minimal 1 (satu) algoritma kriptografi yang terdapat pada SNI ISO/IEC 19790 *annex* C dan *annex* D. 3) Perakitan (*assembling*) Tidak berlaku untuk modul kriptografi berupa perangkat lunak. a) Perakitan dilakukan dengan metode tertentu yang dikendalikan dan memperhatikan Prosedur terkait, keamanan, kesesuaian proses, termasuk kondisi lingkungan kerja, kompetensi SDM, material, peralatan kerja, dan alat pemantauan sesuai dengan

No.	Nama Modul Kriptografi	SNI, Judul SNI	Seleksi	Determinasi	Surveilan	Titik Kritis
	terkait dengan jaringan (*Network and network-related devices and system*); k. Sistem operasi (*Operating systems*); l. Produk untuk tanda tangan digital (*Product for digital signature*); m. Komputasi terpercaya (*Trusted computing*); n. Sistem dan peranti lain (*Other devices and system*).					persyaratan. Proses *assembling* dilakukan sesuai dengan desain Modul Kriptografi. b) Tinjauan kode dilakukan untuk memastikan perangkat lunak mengikuti standar kode dan kontrol keamanan diterapkan. Tes kerentanan keamanan seperti pengujian penetrasi juga dilakukan untuk mengidentifikasi potensi masalah. c) Dilakukan pengaturan konfigurasi keamanan lingkungan yang dikendalikan dan memperhatikan SOP untuk memastikan pembangunan perangkat lunak diterapkan dengan aman. 4) Pengendalian internal mutu Modul Kriptografi (*Quality Assurance*) Pengendalian mutu Modul Kriptografi dilakukan dengan metode tertentu yang dikendalikan, untuk memastikan Modul Kriptografi sesuai dengan persyaratan mutu dan keamanan yang ditetapkan. 5) Penandaan Penandaan dilakukan untuk Modul Kriptografi sesuai dengan persyaratan acuan SNI ISO/IEC 19790:2015 dan peraturan perundangan terkait Keterangan 1. urutan proses produksi setiap Pemohon dapat berbeda; 2. fungsi keamanan pada setiap Modul Kriptografi dapat berbeda.

M. Kriteria Kompetensi Personel atau Tim dalam Kegiatan Sertifikasi

Pengetahuan	Personel yang melakukan tinjauan permohonan	Auditor*	PPC**	Personel yang melakukan tinjauan hasil evaluasi	Pengambil keputusan
Pengetahuan tentang SNI ISO IEC 17065	✓	✓	-	✓	✓
Pengetahuan tentang proses dan prosedur sertifikasi yang ditetapkan oleh lembaga sertifikasi	✓	✓	✓	✓	✓
Pengetahuan dan pengalaman tentang prinsip, praktik, dan teknik audit sesuai SNI ISO 19011	-	✓	-	-	-
Pengetahuan dan pengalaman tentang prinsip, praktik, dan teknik audit sesuai SNI ISO 9001 atau SNI ISO/IEC 27001	-	✓	-	✓	✓
Pengetahuan tentang SNI ISO/IEC 19790:2015	✓	✓	✓	✓	✓
Pengetahuan dan pengalaman tentang sektor bisnis teknologi informasi	-	✓	-	-	✓
Pengetahuan tentang Modul Kriptografi dan proses produksi pembuatan Modul Kriptografi	-	✓	-	-	✓
Pengetahuan pengambilan sampel Modul Kriptografi	-		✓	-	-
Pengetahuan dan pemahaman tentang peraturan perundang-undangan	-	✓		-	-

* Pemenuhan kompetensi dapat dipenuhi secara kolektif dalam satu tim.

** Jika auditor juga bertindak sebagai PPC, maka harus memiliki pengetahuan pengambilan sampel Modul Kriptografi.

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

LAMPIRAN IV
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 11 TAHUN 2024
TENTANG
PENYELENGGARAAN ALGORITMA KRIPTOGRAFI INDONESIA DAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI

PENGGUNAAN TANDA SNI DAN TANDA KMK

A. Tanda SNI dan Tanda KMK
Tanda SNI dan Tanda KMK dicantumkan pada Modul Kriptografi yang telah memperoleh:
1. Sertifikat Keamanan Modul Kriptografi yang dikeluarkan oleh LSPro; dan
2. surat persetujuan penggunaan Tanda SNI dan Tanda KMK yang dikeluarkan dari Kepala Badan.

B. Ketentuan Permohonan Persetujuan Penggunaan Tanda SNI dan Tanda KMK
1. Permohonan persetujuan penggunaan Tanda SNI dan Tanda KMK diajukan secara tertulis oleh LSPro selaku pemohon kepada Kepala Badan.
2. Permohonan tertulis diajukan dengan:
   a. mengisi formulir permohonan penggunaan Tanda SNI dan Tanda KMK
   b. melampirkan salinan Sertifikat Keamanan Modul Kriptografi yang telah dilegalisasi oleh LSPro.
3. Apabila permohonan dinyatakan lengkap, Kepala Badan melalui Deputi melakukan verifikasi permohonan paling lama 5 (lima) hari.
4. Format formulir permohonan penggunaan Tanda SNI dan Tanda KMK sebagai berikut:

LOGO BSSN	FORMULIR PERMOHONAN PENGGUNAAN TANDA SNI DAN TANDA KMK*)	No. Dokumen:	
		No. Revisi:	Tanggal

A. Identitas Pemohon
   1. Lembaga Sertifikasi Produk :
   2. Nomor LPK :
   3. Periode Akreditasi/Penunjukan*) :
   4. Alamat :
   5. Nomor Telepon :
   6. Kontak Person :

B. Calon Pengguna Tanda SNI dan Tanda KMK*)
   1. Data Pemohon*)
      a. Nama perusahaan :
      b. Nomor SIUP :
      c. Alamat :
      d. Nama Pemimpin dan Jabatan :
      e. Nomor Telepon :
      f. Email :
      g. Website :
   2. Data Modul Kriptografi
      a. Merek Modul Kriptografi :
      b. Kategori Modul Kriptografi :
      c. Tipe Modul Kriptografi :
      d. Level Keamanan :
   3. Persyaratan acuan : SNI ISO/IEC 19790:2015

C. Dokumen yang harus dilampirkan
   1. Salinan Sertifikat Keamanan Modul Kriptografi yang telah dilegalisasi oleh LSPro.
   2. Bukti foto jenis Modul Kriptografi ukuran 5R disertai rencana penempatan Tanda SNI dan Tanda KMK.
   3. Legalitas usaha dari calon pengguna Tanda SNI dan Tanda KMK.
   4. Pernyataan surat kuasa dari calon pengguna Tanda SNI dan Tanda KMK.
   5. Surat pernyataan kesediaan mematuhi kewajiban penggunaan Tanda SNI dan Tanda KMK oleh Pemohon.

……,……20..
Pemohon,

(……)

*) coret salah satu

Format Surat pernyataan kesediaan mematuhi kewajiban penggunaan Tanda SNI dan Tanda KMK oleh Pemohon sebagai berikut:

SURAT PERNYATAAN KESEDIAAN MEMATUHI KEWAJIBAN PENGGUNAAN TANDA SNI DAN TANDA KMK

Sehubungan dengan pengajuan permohonan Penggunaan Tanda SNI dan Tanda KMK, dengan ini kami menyatakan bersedia untuk:

1) Menjaga dan mengendalikan kesesuaian barang sebagaimana dimaksud dalam dokumen persetujuan penggunaan Tanda SNI dan Tanda KMK untuk diproduksi atau dipasok sesuai dengan karakteristik yang sama dengan sampel Modul Kriptografi yang telah disertifikasi oleh LSPro serta dinyatakan memenuhi standar yang diacu.
2) Membubuhkan Tanda SNI dan Tanda KMK bagi barang yang dimaksud dalam dokumen persetujuan penggunaan Tanda SNI dan Tanda KMK.
3) Menginformasikan segala perubahan yang dilakukan dan menyebabkan perubahan pemenuhan karakteristik barang dengan karakteristik sampel pada saat dilakukan sertifikasi oleh LPK dalam rangka pemenuhan terhadap standar yang diacu.
4) Menginformasikan segala perubahan lain yang dilakukan yang mempengaruhi dokumen yang disampaikan pada saat pengusulan persetujuan penggunaan Tanda SNI dan Tanda KMK.
5) Mengambil tindakan perbaikan yang diperlukan bila terdapat laporan hasil monitoring atau pengawasan ditemukan ketidakmampuan menjaga dan mengendalikan kesesuaian barang sebagaimana dimaksud dalam dokumen persetujuan penggunaan Tanda SNI dan Tanda KMK.
6) Tidak mencantumkan Tanda SNI dan Tanda KMK pada barang dalam hal Surat Persetujuan Penggunaan Tanda SNI dan Tanda KMK dibekukan, dicabut atau berakhir masa berlakunya.

Tempat,Tanggal:
Pimpinan Pemohon

MATERAI
TTD

Nama :
Jabatan :

5. Berdasarkan hasil verifikasi, Kepala Badan menerbitkan:
   a. surat penolakan; atau
   b. surat persetujuan.
      Format surat persetujuan pengunaan Tanda SNI dan Tanda KMK sebagai berikut:

LOGO BSSN

SURAT PERSETUJUAN PENGGUNAAN TANDA SNI DAN TANDA KMK

Nomor:

Kepala Badan Siber dan Sandi Negara memberikan persetujuan penggunaan Tanda SNI dan Tanda KMK, kepada:

Nama Pemohon	:
Alamat Pemohon	:
Alamat lokasi produksi	:
Merek Modul Kriptografi	:
Kategori Modul Kriptografi	:
Tipe Modul Kriptografi	:
Level Keamanan	:

atas pemenuhan terhadap persyaratan acuan SNI ISO/IEC 19790:2015.

Masa berlaku sampai dengan .....

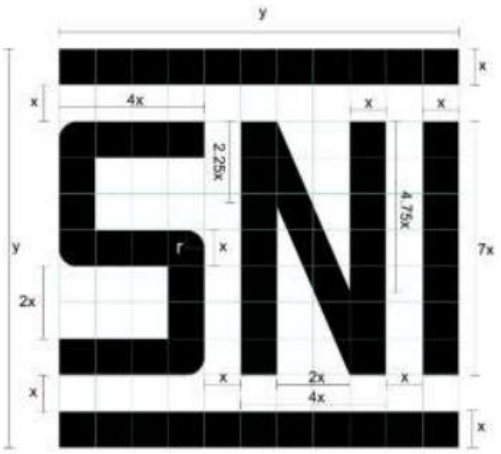
Diterbitkan di : JAKARTA
Pada Tanggal :
Kepala Badan Siber dan Sandi Negara

TTD

(Nama)

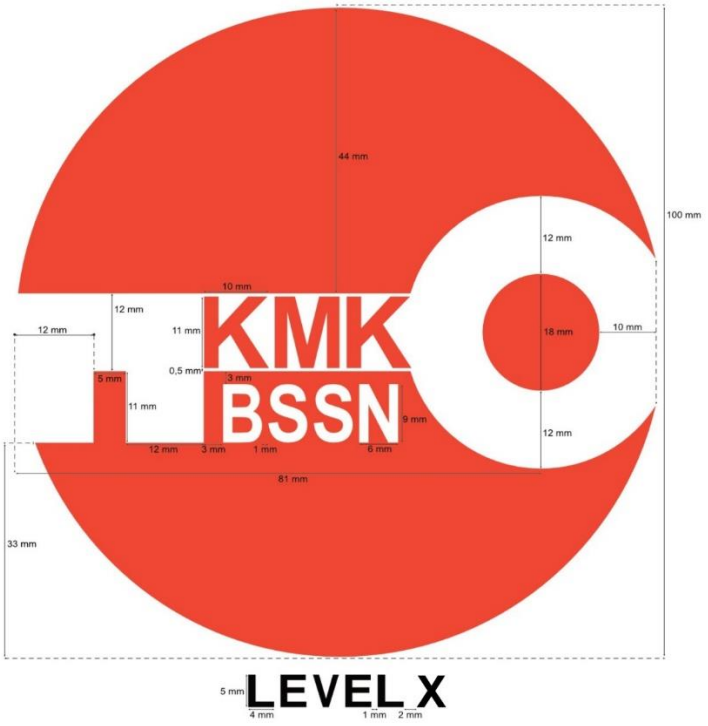
6. Berdasarkan surat persetujuan Kepala Badan, Pemohon berhak mencantumkan Tanda SNI dan Tanda KMK sebagai berikut:

7. Tanda KMK proporsional dan tidak lebih besar dari Tanda SNI.
8. Bentuk, ukuran dan warna Tanda SNI sebagai berikut:



Keterangan:
y = 11x
r = 0,5x

9. Bentuk, ukuran dan warna tanda KMK sebagai berikut:



Keterangan:

a. Bentuk tanda gambar lingkaran dengan gambar kunci, tulisan "KMK", dan "BSSN" berada di dalamnya serta tulisan "LEVEL X" berada di bawah gambar lingkaran
b. Gambar lingkaran berwarna merah (#FA4632)
c. Gambar kunci berwarna putih (#FFFFFF)
d. Tulisan "KMK" ditulis dengan huruf kapital, bercetak tebal, berjenis huruf *Helvetica Now*, dan berwarna merah (#FA4632)

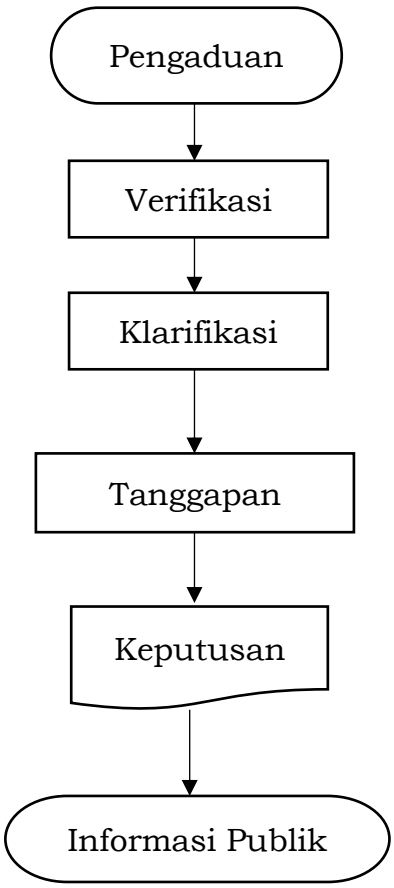
e. Tulisan “BSSN” ditulis dengan huruf kapital, bercetak tebal, berjenis huruf *Arial*, dan berwarna putih (#FFFFFF)
f. Tulisan “LEVEL X” ditulis dengan huruf kapital, berjenis huruf *Arial*, dan berwarna hitam (#000000), huruf “X” dapat diganti dengan angka yang merupakan Level Keamanan Modul Kriptografi yaitu 2 (dua) s.d. 4 (empat)
g. Diperbolehkan menggunakan warna hitam putih ataupun monokrom
h. Setiap pembesaran atau pengecilan ukuran tanda KMK harus proporsional dengan tanda yang digunakan sebagai acuan.

10. Berikut contoh Tanda SNI dan Tanda KMK pada Modul Kriptografi dengan Level Keamanan 3:

11. Penggunaan Tanda SNI dan Tanda KMK berlaku selama 5 (lima) tahun
12. Kepala Badan melalui Deputi mengumumkan setiap persetujuan permohonan penggunaan Tanda SNI dan Tanda KMK melalui situs Badan.
13. Pengumuman memuat informasi paling sedikit:
    a. identitas Modul Kriptografi;
    b. identitas Pemohon;
    c. nomor surat persetujuan penggunaan Tanda SNI dan Tanda KMK;
    d. masa berlaku penggunaan Tanda SNI dan Tanda KMK; dan
    e. identitas LSPro.
14. Pembubuhan Tanda SNI dan Tanda KMK sebagai berikut:
    a. Tanda SNI dan Tanda KMK ditampilkan pada Modul Kriptografi dan/atau pada kemasan terkecil, apabila tidak memungkinkan, Tanda SNI dan Tanda KMK ditampilkan pada kemasan yang lebih besar sedemikian rupa sehingga mudah dilihat oleh pembeli atau pengguna. Penggunaan Tanda SNI dan Tanda KMK harus dengan pencetakan yang permanen di Modul Kriptografi atau kemasannya.
    b. Tanda SNI dan Tanda KMK yang tidak memungkinkan ditampilkan pada Modul Kriptografi, dapat ditampilkan dalam media lain (misal: brosur, situs web, dan sebagainya, yang tidak menyebabkan salah pengertian.

C. Pembinaan dan Pengawasan Penggunaan Tanda SNI dan Tanda KMK
Kepala Badan melalui Deputi melakukan pembinaan dan pengawasan terhadap penggunaan Tanda SNI dan Tanda KMK.

D. Pengaduan Masyarakat
1. Apabila mengetahui adanya penyalahgunaan terhadap penggunaan Tanda SNI dan Tanda KMK, masyarakat dapat mengajukan pengaduan kepada Kepala Badan.
2. Pengaduan disampaikan secara tertulis dengan mengisi formulir pengaduan.
3. Tata cara pengaduan sebagai berikut:



Keterangan:
a. Pelapor menyampaikan pengaduan tentang terjadinya penyalahgunaan penggunaan Tanda SNI dan Tanda KMK kepada Kepala Badan sesuai format yang telah disediakan.
b. Kepala Badan melalui Deputi melakukan verifikasi terhadap isi pengaduan.
c. Kepala Badan melalui Deputi meminta klarifikasi kepada:
   1) Pemohon, apabila penggunaan Tanda SNI dan Tanda KMK tanpa melalui proses sertifikasi; dan/atau
   2) LSPro, apabila penggunaan Tanda SNI dan Tanda KMK melalui proses sertifikasi.
d. Pemohon, LSPro memberikan tanggapan kepada Kepala Badan.
e. Berdasarkan hasil tanggapan dari Pemohon atau LSPro, apabila:
   1) pengaduan tidak terbukti, Kepala Badan menyampaikan hasil tanggapan kepada pelapor.
   2) pengaduan terbukti, Kepala Badan menerbitkan surat teguran untuk mencabut penggunaan Tanda SNI dan Tanda KMK.

f. Kepala Badan mengumumkan keputusan hasil pengaduan kepada publik dan pelapor.

4. Format formulir pengaduan penyalahgunaan penggunaan Tanda SNI dan Tanda KMK sebagai berikut:

FORMULIR PENGADUAN PENYALAHGUNAAN
PENGGUNAAN TANDA SNI DAN TANDA KMK

Data Pelapor
1. Nama :
2. Alamat :
3. Email :
4. Telepon :

Data Aduan
1. Nama Modul Kriptografi :
2. Lokasi Modul Kriptografi :
3. Tanggal :
4. Isi Aduan :

Pengaduan ini saya buat dengan sebenar-benarnya dan saya bertanggung jawab sepenuhnya terhadap isi pengaduan.

……,……20..
Pelapor,

(……)

5. Apabila pengaduan terbukti, Pemohon yang melanggar ketentuan dikenai sanksi sesuai dengan peraturan perundang-undangan disertai pencabutan persetujuan penggunaan Tanda SNI dan Tanda KMK.

E. Biaya
Permohonan penggunaan Tanda SNI dan Tanda KMK tidak dikenakan biaya.

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

LAMPIRAN V
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 11 TAHUN 2024
TENTANG
PENYELENGGARAAN ALGORITMA KRIPTOGRAFI INDONESIA DAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI

PENYELENGGARA SKEMA PKKMK UNTUK MODUL KRIPTOGRAFI YANG MERUPAKAN TEKNOLOGI PELINDUNGAN IIV

A. Pemilik Skema Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV

Pemilik Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV yaitu Kepala Badan yang memiliki tanggung jawab sebagai berikut:

1. menetapkan Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV;
2. menetapkan rencana strategis Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV
3. memberikan persetujuan penggunaan Tanda SNI dan Tanda KMK;
4. menetapkan LSPro dan laboratorium pengujian untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV;
5. menetapkan peraturan lain sesuai dengan kewenangannya.

B. Komite Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV

Komite Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV terdiri atas:

1. Deputi; dan
2. Direktur.

Tanggung Jawab Komite Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV sebagai berikut:

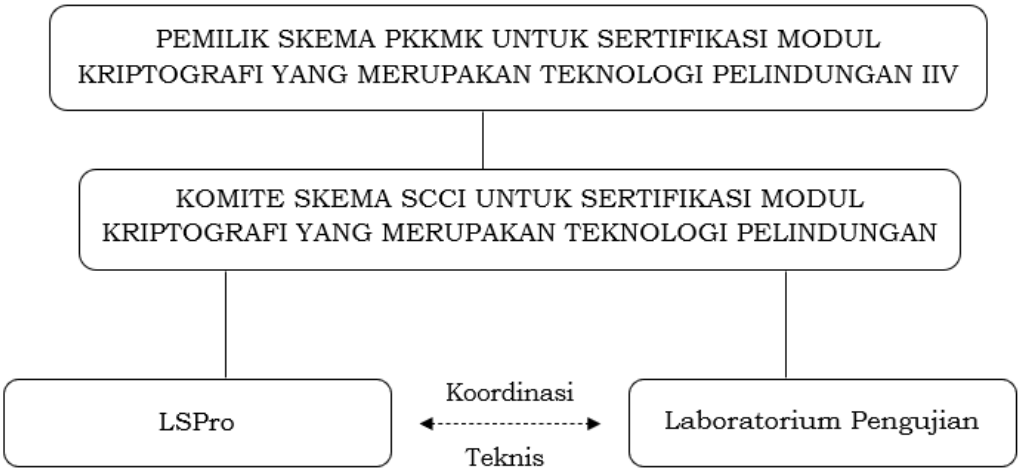
1. memberikan arahan strategis pelaksanaan Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV;
2. mengomunikasikan arah strategis manajemen kebijakan Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV;
3. merumuskan Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV;
4. merumuskan kebijakan penggunaan Tanda SNI dan Tanda KMK;
5. melakukan pengawasan dan pengendalian terhadap implementasi Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV;
6. melaksanakan evaluasi Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV paling sedikit 24 (dua puluh empat) bulan sejak pelaksanaan evaluasi sebelumnya, atau dapat diubah dengan ketentuan sebagai berikut:

a. terdapat perubahan persyaratan acuan yang digunakan pada Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV;
b. adanya perubahan struktur organisasi dan/atau tugas dan fungsi Badan; dan/atau
c. adanya rekomendasi kaji ulang Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV.

C. LSPro
1. LSPro ditetapkan oleh Kepala Badan sebagai LSPro.
2. LSPro memiliki tugas melaksanakan sertifikasi produk sesuai dengan persyaratan acuan SNI ISO/IEC 19790:2015.
3. LSPro paling sedikit terdiri atas:
   a. kepala;
   b. peninjau sertifikasi terdiri atas paling sedikit 1 (satu) orang anggota LSPro yang tidak terlibat dalam proses evaluasi;
   c. manajer teknis;
   d. manajer mutu;
   e. 4 (empat) orang auditor; dan
   f. petugas pengambil contoh.

D. Laboratorium Pengujian untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV
1. Laboratorium Pengujian diselenggarakan oleh pemerintah atau swasta.
2. Laboratorium Pengujian ditunjuk dan ditetapkan oleh Kepala Badan sesuai dengan ketentuan peraturan perundang-undangan.
3. Laboratorium Pengujian memiliki tugas melakukan pengujian kesesuaian keamanan Modul Kriptografi berdasarkan Skema PKKMK.
4. Laboratorium Pengujian paling sedikit terdiri atas:
   a. kepala;
   b. manajer teknis;
   c. manajer mutu; dan
   d. 4 (empat) orang evaluator

E. Struktur penyelenggara Skema PKKMK untuk Modul Kriptografi yang merupakan teknologi pelindungan IIV sebagaimana yang ditunjukan pada Gambar 1.



Gambar 1 Struktur penyelenggara Skema Penilaian Kesesuaian Keamanan Modul Kriptografi

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

LAMPIRAN VI
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 11 TAHUN 2024
TENTANG
PENYELENGGARAAN ALGORITMA KRIPTOGRAFI INDONESIA DAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI

TATA CARA PENUNJUKAN DAN PENGAWASAN LSPRO DAN LABORATORIUM PENGUJIAN

A. Penunjukan LSPro
Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara Pasal 2 yang menyatakan bahwa BSSN mempunyai tugas melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan. Dalam rangka pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi dan sebagai salah satu bentuk pelaksanaan Pasal 3, maka BSSN membentuk satu unit kerja yang mempunyai tugas dan fungsi di bidang pengujian dan sertifikasi produk keamanan siber dan sandi yaitu lembaga sertifikasi produk BSSN. Oleh karena itu untuk melaksanakan amanat Peraturan Presiden Nomor 28 Tahun 2021, Kepala Badan menunjuk lembaga sertifikasi BSSN sebagai LSPro.

B. Tata Cara Penunjukan laboratorium pengujian
1. Kepala Badan melalui Deputi menerbitkan surat edaran kepada lembaga penilai kesesuaian perihal penunjukan laboratorium pengujian.
2. Penunjukan laboratorium pengujian dilaksanakan oleh Badan melalui Deputi berkoordinasi dengan KAN dan kementerian terkait.
3. Laboratorium pengujian yang dapat ditunjuk Kepala Badan harus memenuhi kriteria yang meliputi:
   a. identitas laboratorium pengujian berupa perizinan berusaha di bidang industri jasa pengujian laboratorium yang efektif atau penetapan tugas dan fungsi kelembagaan bagi laboratorium pengujian yang dimiliki oleh pemerintah sesuai dengan ketentuan peraturan perundangan-undangan;
   b. berdomisili atau berkedudukan di wilayah Republik Indonesia; dan
   c. telah diakreditasi oleh KAN untuk lingkup yang sesuai.
4. Laboratorium pengujian mengajukan permohonan kepada Kepala Badan dilengkapi dokumen pendukung yang meliputi:
   a. dokumen perizinan berusaha di bidang industri jasa pengujian laboratorium yang efektif atau peraturan perundang-undangan mengenai penetapan tugas dan fungsi kelembagaan bagi laboratorium pengujian yang dimiliki oleh pemerintah;
   b. dokumen struktur organisasi laboratorium pengujian;

c. sertifikat akreditasi KAN dan lampirannya untuk lingkup yang sesuai;
d. daftar sumber daya yang dimiliki; antara lain daftar dan kompetensi personel; sarana dan prasarana; dan
e. daftar pengalaman dan kemampuan laboratorium pengujian dalam pelaksanaan pengujian untuk ruang lingkup yang sejenis selama 2 (dua) tahun terakhir.

5. Deputi melalui direktorat yang melaksanakan tugas dan fungsi di bidang koordinasi, perumusan dan pemantauan kebijakan teknis di bidang teknologi keamanan siber, melakukan verifikasi kelengkapan permohonan penunjukan laboratorium pengujian.
6. Apabila laboratorium pengujian tidak memenuhi persyaratan maka Deputi menyampaikan pemberitahuan kepada laboratorium pengujian untuk melengkapi dokumen dalam waktu paling lama 5 (lima) hari kerja. Dalam hal laboratorium pengujian tidak melengkapi dokumen sebagaimana waktu yang ditentukan maka permohonan dianggap batal.
7. Jika laboratorium pengujian memenuhi persyaratan, maka Deputi membentuk tim verifikasi dan tim penilai.
8. Tim verifikasi melakukan verifikasi lapangan terhadap laboratorium pengujian yang memenuhi persyaratan sesuai dengan prosedur yang berlaku.

   Tim verifikasi berasal dari perwakilan direktorat yang melaksanakan tugas dan fungsi koordinasi, perumusan, dan pemantauan kebijakan teknis di bidang teknologi keamanan siber yang memenuhi kriteria sebagai berikut:
   a. ketua tim harus:
      1) memiliki pengetahuan tentang SNI ISO 9001 atau SNI ISO/IEC 27001 dan SNI ISO/IEC 17025 yang dibuktikan dengan sertifikat pelatihan atau bukti lain yang sejenis;
      2) memiliki pengetahuan tentang SNI ISO/IEC 19790:2015 yang dibuktikan dengan sertifikat pelatihan atau bukti lain yang sejenis;
      3) berpengalaman kerja pada bidangnya dibuktikan dengan daftar riwayat hidup; dan
      4) minimal pejabat fungsional ahli muda.
   b. wakil ketua dan anggota harus:
      1) memiliki pengetahuan tentang SNI ISO 9001 atau SNI ISO/IEC 27001 dan SNI ISO/IEC 17025 yang dibuktikan dengan sertifikat pelatihan atau bukti lain yang sejenis;
      2) memiliki pengetahuan tentang SNI ISO/IEC 19790:2015 yang dibuktikan dengan sertifikat pelatihan atau bukti lain yang sejenis; dan
      3) berpengalaman kerja pada bidangnya dibuktikan dengan daftar riwayat hidup.
9. Tim penilai melaksanakan penilaian berdasarkan hasil verifikasi kelengkapan permohonan dan hasil verifikasi lapangan sesuai dengan prosedur yang berlaku.

Tim penilai berasal dari perwakilan direktorat yang melaksanakan tugas dan fungsi di bidang koordinasi, perumusan, dan pemantauan kebijakan teknis di bidang teknologi keamanan siber yang memenuhi kriteria sebagai berikut:

a. ketua tim harus:
   1) memiliki pengetahuan tentang SNI ISO 9001 atau SNI ISO/IEC 27001 dan SNI ISO/IEC 17025 yang dibuktikan dengan sertifikat pelatihan atau bukti lain yang sejenis;
   2) memiliki pengetahuan tentang SNI ISO/IEC 19790:2015 yang dibuktikan dengan sertifikat pelatihan atau bukti lain yang sejenis;
   3) memiliki kompetensi spesifik atas Modul Kriptografi yang dibahas dan berpengalaman kerja pada bidangnya dibuktikan dengan daftar riwayat hidup; dan
   4) minimal pejabat fungsional ahli madya.
b. wakil ketua dan anggota harus:
   1) memiliki pengetahuan tentang SNI ISO 9001 atau SNI ISO/IEC 27001 dan SNI ISO/IEC 17025 yang dibuktikan dengan sertifikat pelatihan atau bukti lain yang sejenis;
   2) memiliki pengetahuan tentang SNI ISO/IEC 19790:2015 yang dibuktikan dengan sertifikat pelatihan atau bukti lain yang sejenis; dan
   3) memiliki kompetensi spesifik atas Modul Kriptografi yang dibahas dan berpengalaman kerja pada bidangnya dibuktikan dengan daftar riwayat hidup.

10. Berdasarkan hasil penilaian, Kepala Badan dapat menyetujui atau menolak permohonan penunjukan laboratorium pengujian.
    a. Dalam hal permohonan disetujui, Kepala Badan menerbitkan surat penunjukan laboratorium pengujian.
    b. Dalam hal permohonan penunjukan lembaga penilaian kesesuaian ditolak, Kepala Badan memberitahukan secara tertulis kepada lembaga penilaian kesesuaian disertai dengan alasan penolakan.
11. Format surat penunjukan laboratorium pengujian sebagai berikut:

KEPALA BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA
NOMOR:

TENTANG
PENUNJUKAN LEMBAGA SERTIFIKASI PRODUK DAN/ATAU LABORATORIUM PENGUJIAN*)
DALAM RANGKA PENYELENGGARAAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI YANG MERUPAKAN TEKNOLOGI PELINDUNGAN IIV

KEPALA BADAN SIBER DAN SANDI NEGARA

Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal ... Peraturan Badan Siber dan Sandi Negara Nomor ... Tahun ... tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi perlu ditunjuk Lembaga Sertifikasi Produk dan/atau Laboratorium Pengujian)* dalam rangka penilaian kesesuaian keamanan Modul Kriptografi yang merupakan teknologi pelindungan Infrastruktur Informasi Vital untuk mendukung penerapan domain pada kerangka kerja pelindungan Infrastruktur Informasi Vital;

b. bahwa penunjukan Lembaga Sertifikasi Produk dan/atau Laboratorium Pengujian)* dalam rangka penilaian kesesuaian keamanan Modul Kriptografi yang merupakan teknologi pelindungan Infrastruktur Informasi Vital merupakan Lembaga Sertifikasi Produk dan/atau Laboratorium Pengujian)* yang telah diakreditasi untuk ruang lingkup yang sesuai;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan b, perlu menetapkan Keputusan Kepala Badan Siber dan Sandi Negara tentang Penunjukan Lembaga Sertifikasi Produk dan/atau Laboratorium Pengujian)* dalam rangka penyelenggaraan penilaian kesesuaian keamanan Modul Kriptografi.

Mengingat	:	1. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803) sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan Atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2023 Nomor 544); 2. Peraturan Badan Siber dan Sandi Negara Nomor ... Tahun ... tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penyelenggaraan Penilaian Kesesuaian Keamanan Modul Kriptografi (Berita Negara Republik Indonesia Tahun ... Nomor ...);
		MEMUTUSKAN
Menetapkan	:	KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA TENTANG PENUNJUKAN LEMBAGA SERTIFIKASI PRODUK DAN/ATAU LABORATORIUM PENGUJIAN)* DALAM RANGKA PENYELENGGARAAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI YANG MERUPAKAN TEKNOLOGI PELINDUNGAN IIV.
KESATU	:	Menunjuk Lembaga Sertifikasi Produk dan/atau Laboratorium Pengujian)* dalam rangka penyelenggaraan penilaian kesesuaian keamanan Modul Kriptografi Indonesia sebagaimana tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan Kepala ini.
KEDUA	:	Penunjukan Lembaga Sertifikasi Produk dan/atau Laboratorium Pengujian)* sebagaimana dimaksud dalam Diktum KESATU berlaku untuk jangka waktu 5 (tahun) tahun.
KETIGA	:	Badan Siber dan Sandi Negara melalui unit kerja yang menyelenggarakan fungsi pelaksanaan pemantauan, evaluasi, dan pelaporan di bidang sistem dan strategi keamanan siber dan sandi secara berkala atau sewaktu-waktu melakukan pengawasan terkait pelaksanaan penyelenggaraan penilaian kesesuaian keamanan Modul Kriptografi kepada Lembaga Sertifikasi Produk dan/atau Laboratorium Pengujian)*.

KEEMPAT	:	Lembaga Sertifikasi Produk dan/atau Laboratorium Pengujian)* sebagaimana dimaksud dalam Diktum KESATU wajib menyampaikan laporan setiap 1 (satu) tahun kepada Kepala Badan yang berisi perkembangan penyelenggaraan penilaian kesesuaian keamanan Modul Kriptografi.
KELIMA	:	Keputusan Kepala ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
Pada tanggal

KEPALA BADAN SIBER DAN SANDI NEGARA,

(*tanda tangan*)

(*nama lengkap*)

Keterangan:
*) Pilih salah satu

LAMPIRAN KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA
NOMOR :
TANGGAL :

LEMBAGA SERTIFIKASI PRODUK DAN/ATAU LABORATORIUM PENGUJIAN*)
UNTUK PENYELENGGARAAN PENILAIAN KESESUAIAN KEAMANAN MODUL KRIPTOGRAFI YANG MERUPAKAN TEKNOLOGI PELINDUNGAN IIV

No.	Nama LSPro/ Laboratorium Pengujian*)	Alamat	Keterangan
1.			
dst.			

KEPALA BADAN SIBER DAN SANDI NEGARA,

(*tanda tangan*)

(*nama lengkap*)

Keterangan:
*) Pilih salah satu

C. Pengawasan LSPro
1. Deputi melalui direktorat yang melaksanakan tugas dan fungsi di bidang koordinasi, perumusan, dan pemantauan kebijakan teknis di bidang teknologi keamanan siber melaksanakan pengawasan terhadap LSPro.
2. Pengawasan terhadap LSPro dilaksanakan secara berkala dan/atau khusus.
3. Pengawasan secara berkala dilaksanakan 1 (satu) kali dalam 1 (satu) tahun melalui evaluasi laporan perkembangan sertifikasi yang disampaikan oleh laboratorium pengujian kepada Kepala Badan melalui Deputi.
4. Laporan perkembangan sertifikasi yang disampaikan LSPro paling sedikit meliputi:
   a. profil LSPro termutakhir minimal terdiri atas:
      1) identitas LSPro meliputi nama, alamat, nomor telepon, nama personel penghubung;
      2) akreditasi LSPro meliputi nomor akreditasi lembaga sertifikasi produk, lingkup akreditasi dan masa berlaku akreditasi;
      3) struktur organisasi LSPro; dan

4) daftar dan kompetensi personel LSPro.

b. laporan tahunan penerbitan, pengawasan, pencabutan atau perubahan sertifikat penilaian kesesuaian dengan disertai lampiran salinan sertifikat penilaian kesesuaian yang diterbitkan

5. Pengawasan secara khusus terhadap LSPro dilaksanakan apabila terdapat pengaduan. Penanganan pengaduan dilakukan sesuai dengan prosedur yang berlaku.
6. Hasil pengawasan menjadi rekomendasi bagi Kepala Badan dalam pengambilan keputusan terkait pengenaan sanksi terhadap LSPro yang bersangkutan.

D. Pengawasan laboratorium pengujian

1. Deputi melalui direktorat yang melaksanakan tugas dan fungsi di bidang koordinasi, perumusan, dan pemantauan kebijakan teknis di bidang teknologi keamanan siber melaksanakan pengawasan terhadap laboratorium pengujian.
2. Pengawasan terhadap laboratorium pengujian dilaksanakan secara berkala dan/atau khusus.
3. Pengawasan secara berkala dilaksanakan 1 (satu) kali dalam 1 (satu) tahun melalui evaluasi laporan perkembangan pengujian yang disampaikan oleh laboratorium pengujian kepada Kepala Badan melalui Deputi.
4. Laporan perkembangan pengujian yang disampaikan laboratorium pengujian paling sedikit meliputi:
   a. Profil laboratorium pengujian termutakhir minimal terdiri atas:
      1) identitas laboratorium pengujian meliputi nama, alamat, nomor telepon, nama personel penghubung;
      2) akreditasi laboratorium pengujian meliputi nomor akreditasi laboratorium pengujian, lingkup akreditasi dan masa berlaku akreditasi;
      3) struktur organisasi laboratorium pengujian;
      4) daftar dan kompetensi personel laboratorium pengujian; dan
      5) daftar fasilitas pengujian.
   b. laporan tahunan penerbitan laporan hasil uji disertai lampiran laporan hasil uji yang diterbitkan.
5. Pengawasan secara khusus terhadap laboratorium pengujian dilaksanakan apabila terdapat pengaduan. Penanganan pengaduan dilakukan sesuai dengan prosedur yang berlaku.
6. Hasil pengawasan menjadi rekomendasi bagi Kepala Badan dalam pengambilan keputusan terkait pengenaan sanksi terhadap laboratorium pengujian yang bersangkutan.
7. Sanksi terhadap laboratorium pengujian dilaksanakan melalui pembekuan atau pencabutan surat penunjukan laboratorium pengujian atau sebagian ruang lingkup pengujian yang ditetapkan.
8. Pembekuan atau pencabutan surat penunjukan laboratorium pengujian atau sebagian ruang lingkup pengujian yang ditetapkan dilakukan oleh Kepala Badan melalui Deputi.
9. Laboratorium pengujian yang surat penunjukannya dibekukan, dapat mengajukan permohonan pengaktifan kembali surat penunjukannya

dengan menunjukkan bukti bahwa hal yang menyebabkan pembekuannya telah terpenuhi.

10. Laboratorium pengujian yang surat penunjukan laboratorium pengujian atau sebagian ruang lingkup pengujiannya dicabut, hanya dapat mengajukan permohonan penunjukkan sebagai laboratorium pengujian setelah 1 (satu) tahun sejak tanggal pencabutan.
11. Permohonan pengaktifan disampaikan kepada Kepala Badan melalui Deputi.
12. Kepala Badan melalui Deputi melakukan evaluasi terhadap permohonan pengaktifan kembali surat penunjukan laboratorium pengujian.
13. Berdasarkan hasil evaluasi, Kepala Badan dapat menyetujui atau menolak permohonan pengaktifan kembali surat penunjukan laboratorium pengujian.

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN