MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 4 TAHUN 2023
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA
KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK
TELEKOMUNIKASI BIDANG KRIPTOGRAFI

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal 31 Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia, perlu menetapkan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Telekomunikasi Bidang Kriptografi;

b. bahwa Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Telekomunikasi Bidang Kriptografi telah disepakati melalui Konvensi Nasional pada 26 September 2022 di Jakarta;

c. bahwa sesuai surat Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi, Badan Siber dan Sandi Negara Nomor 5279/BSSN/D1/PS.02.01/11/2022 tanggal 22 November 2022 perihal permohonan Penetapan Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Telekomunikasi Bidang Kriptografi;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Keputusan Menteri Ketenagakerjaan tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Kategori Informasi dan Komunikasi Golongan Pokok Telekomunikasi Bidang Kriptografi;

Mengingat : 1. Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 39, Tambahan Lembaran Negara Republik Indonesia Nomor 4279);

2. Peraturan Pemerintah Nomor 31 Tahun 2006 tentang Sistem Pelatihan Kerja Nasional (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 67, Tambahan Lembaran Negara Republik Indonesia Nomor 4637);

3. Peraturan Presiden Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 24);

4. Peraturan Presiden Nomor 95 Tahun 2020 tentang Kementerian Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 213);

5. Peraturan Menteri Ketenagakerjaan Nomor 21 Tahun 2014 tentang Pedoman Penerapan Kerangka Kualifikasi Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2014 Nomor 1792);

6. Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 258);

7. Peraturan Menteri Ketenagakerjaan Nomor 1 Tahun 2021 tentang Organisasi dan Tata Kerja Kementerian Ketenagakerjaan (Berita Negara Republik Indonesia Tahun 2021 Nomor 108);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN MENTERI KETENAGAKERJAAN TENTANG PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK TELEKOMUNIKASI BIDANG KRIPTOGRAFI.

KESATU : Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Telekomunikasi Bidang Kriptografi, sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Menteri ini.

KEDUA : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

KETIGA : Pemberlakuan Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dan penyusunan jenjang kualifikasi nasional sebagaimana dimaksud dalam Diktum KEDUA ditetapkan oleh Badan Siber dan Sandi Negara dan/atau kementerian/lembaga teknis terkait sesuai dengan tugas dan fungsinya.

KEEMPAT : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dikaji ulang setiap 5 (lima) tahun atau sesuai dengan kebutuhan.

KELIMA : Keputusan Menteri ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 16 Januari 2023

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH

LAMPIRAN
KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 4 TAHUN 2023
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK TELEKOMUNIKASI BIDANG KRIPTOGRAFI

BAB I
PENDAHULUAN

A. Latar Belakang

Pada abad ke-18, Napoleon Bonaparte menyatakan bahwa "*war is ninety percent information*", yang dapat dimaknai bahwa informasi merupakan kunci untuk memenangkan suatu peperangan. Kutipan tersebut merujuk pada informasi tentang kondisi lawan dan kemampuan atau sumber daya yang dimiliki untuk merespon. Informasi yang diperoleh menjadi bahan pertimbangan dalam menetapkan prioritas, memahami risiko, menetapkan sumber daya, menemukan ancaman, menyelidiki insiden, mengotomatiskan tindakan, dan sebagainya. Perbedaan besar antara abad ke-19 dan abad ke-21 adalah kemampuan dalam mengumpulkan dan menganalisis informasi secara instan. Saat ini, cukup dengan menekan satu tombol saja, maka hampir seluruh informasi yang diperlukan dapat diperoleh dengan mudah.

Seiring dengan evolusi informasi dan komunikasi, tidak dapat ditampik bahwa perkembangan sistem telekomunikasi telah berkembang dari jaringan telekomunikasi yang berbasis *circuit switching* dengan pola yang terpusat, menjadi jaringan komunikasi berbasis sistem komputer yang terdistribusi dalam konteks global (internet). Saat ini, internet menjadi keniscayaan media global karena kecepatan dan kemudahan dalam penggunaannya. Akses terhadap internet pun diyakini sebagai salah satu hak asasi manusia yang wajib dipenuhi oleh pemerintah. Sejalan dengan transformasi digital dan *Internet of Things* (IoT), internet kini menjadi faktor penting dalam kehidupan bermasyarakat, berbangsa, dan bernegara. Selain berhak menggunakan internet, setiap orang juga

berhak mendapat perlindungan sedemikian rupa sehingga tidak menimbulkan benturan dengan hak orang lain. Perlindungan yang dimaksud ini dapat diperoleh melalui penerapan kriptografi.

Kriptografi berasal dari kata *kriptos* dan *graphia*. *Kriptos* berarti sesuatu yang dirahasiakan, sedangkan *graphia* berarti tulisan. Oleh karena itu kriptografi secara bahasa berarti tulisan yang dirahasiakan. Menurut Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone dalam buku mereka yang berjudul *Handbook of Applied Cryptography* menyebutkan bahwa kriptografi adalah teknik matematika yang berhubungan dengan aspek keamanan seperti kerahasiaan data, integritas data dan keabsahan data.

Selama beberapa dekade terakhir, kriptografi dikenal sebagai metode yang dapat memenuhi empat aspek keamanan yang terdiri atas kerahasiaan, integritas, autentikasi dan kenirsangkalan. Keempat aspek ini dapat dipenuhi secara bersama-sama dalam suatu sistem atau hanya satu dan sebagian sesuai dengan kebutuhan layanan yang dihasilkan oleh sistem. Kerahasiaan merupakan aspek keamanan yang menjadi ciri khas kriptografi. Dengan menggunakan teknik enkripsi, suatu data atau informasi ditransformasikan agar tidak dapat dibaca atau diakses secara tidak sah.

Aspek keamanan kedua yang dapat dipenuhi oleh kriptografi adalah integritas. Integritas mengacu pada metode atau langkah-langkah untuk menjaga agar data atau informasi tidak dapat dimanipulasi, diubah, atau diedit oleh entitas yang tidak berwenang. Integritas tidak hanya melindungi keakuratan data atau informasi namun juga mencegah perubahan informasi yang tidak disengaja. Hal ini dimungkinkan melalui penerapan *hash function*.

Yang ketiga, kriptografi dapat memenuhi kebutuhan sistem terhadap pengaturan hak akses melalui autentikasi. Autentikasi adalah suatu metode untuk menentukan bahwa entitas/*user* yang akan mengakses sistem adalah asli atau benar. Selain itu autentikasi juga merupakan salah satu dari banyak metode yang dapat digunakan untuk membuktikan bahwa dokumen tertentu yang diterima adalah dari entitas yang benar. Autentikasi dapat dilakukan dengan metode *something you*

know (sesuatu yang diketahui, misalkan: PIN dan *password*), *something you have* (sesuatu yang dimiliki, misalkan: token, *digital certificate*, dan *smartcard*), *who you are* (siapa dirimu, misalkan: *biometric*), dan *something you do* (sesuatu yang dilakukan, misalkan: *input captcha*). Terakhir, kriptografi dapat memenuhi aspek kenirsangkalan yang memastikan entitas tidak dapat menyangkal setiap aksi yang dilakukan dalam sistem.

Selanjutnya, dengan berkembangnya metode dan keilmuan di bidang kriptografi, maka aspek keamanan yang dapat dipenuhi melalui kriptografi menjadi semakin berkembang. Diantaranya adalah ketersediaan data, akuntabilitas, dan otorisasi. Kriptografi dapat mendukung ketersediaan data dengan menjamin bahwa entitas yang berhak dapat menggunakan sistem dan/atau mengambil data dengan cara yang dapat diandalkan dan tepat waktu. Hal ini dilakukan untuk memastikan bahwa sistem informasi dapat diandalkan dan dapat diakses. Selain perangkat keras dan perangkat lunak, juga diperlukan perlindungan dari proses penghapusan dan gangguan, termasuk serangan *Denial of Service* (DOS) yang melumpuhkan layanan sistem.

Kriptografi juga mendukung tercapainya aspek akuntabilitas dalam sistem. Hal ini dimungkinkan karena kriptografi menyediakan suatu kontrol yang memastikan bahwa tindakan entitas dapat dilacak secara unik terhadap entitas tersebut. Apabila suatu sistem memenuhi aspek akuntabilitas, maka secara langsung juga sudah mendukung terpenuhinya aspek nirsangkal (*non-repudiation*), pencegahan, isolasi kesalahan (*fault isolation*), serta tindakan pemulihan insiden dan tindakan hukum.

Aspek keamanan lain yang dapat dipenuhi oleh kriptografi adalah otorisasi. Otorisasi adalah mekanisme pengaturan terkait hak atau izin yang diberikan kepada suatu entitas untuk mengakses sumber daya sistem. Otorisasi dipenuhi melalui mekanisme pengendalian akses yang membatasi akses terhadap perangkat keras, perangkat lunak, dan informasi. Mekanisme otorisasi biasanya digunakan bersamaan dengan autentikasi yang dapat dilihat sebagai struktur akses suatu sistem.

Merujuk pada penjelasan di atas, maka dapat disimpulkan bahwa aspek keamanan yang dapat dipenuhi dengan penerapan kriptografi

menjadi semakin luas menjadi kerahasiaan, autentikasi, ketersediaan, keutuhan, akuntabilitas, dan otorisasi. Berbagai aspek keamanan ini sangat diperlukan penerapannya di era transformasi digital. Di Indonesia, hal ini dapat dilihat pada program transformasi digital yang salah satunya mendorong penerapan sertifikat elektronik untuk berbagai keperluan diantaranya untuk penerbitan dokumen kependudukan, sertifikat kepemilikan tanah, perpajakan, serta proses penandatanganan berbagai dokumen elektronik di berbagai organisasi.

Karenanya, tidak salah jika disimpulkan bahwa kriptografi merupakan jantung keamanan siber. Hal ini selaras dengan apa yang disampaikan oleh Keith M. Martin bahwa *"Cryptography lies at the heart of all cybersecurity technologies, and appreciating the role it plays is vital to understanding how to secure cyberspace"*. Dengan demikian penerapan kriptografi merupakan suatu keniscayaan dan pengembangannya akan turut serta mendorong tingkat keamanan di dunia siber (*cyberspace*).

Berdasarkan data dari *Menlo Security* pada Tahun 2021, Indonesia memiliki 202 juta pengguna internet. Jumlah ini berkontribusi sekitar US$70 miliar terhadap ekonomi digital nasional pada 2021, dengan US$146 miliar diproyeksikan pada Tahun 2025. Ekonomi digital disebut menjadi kunci masa depan ekonomi dunia dan menjadi pilar utama dengan kontribusi 15,5% pada Produk Domestik Bruto (PDB) global. Namun, jika keamanan siber tidak terjaga, kebocoran data akibat kejahatan siber berpotensi menimbulkan kerugian ekonomi hingga US$ 5 triliun pada Tahun 2024.

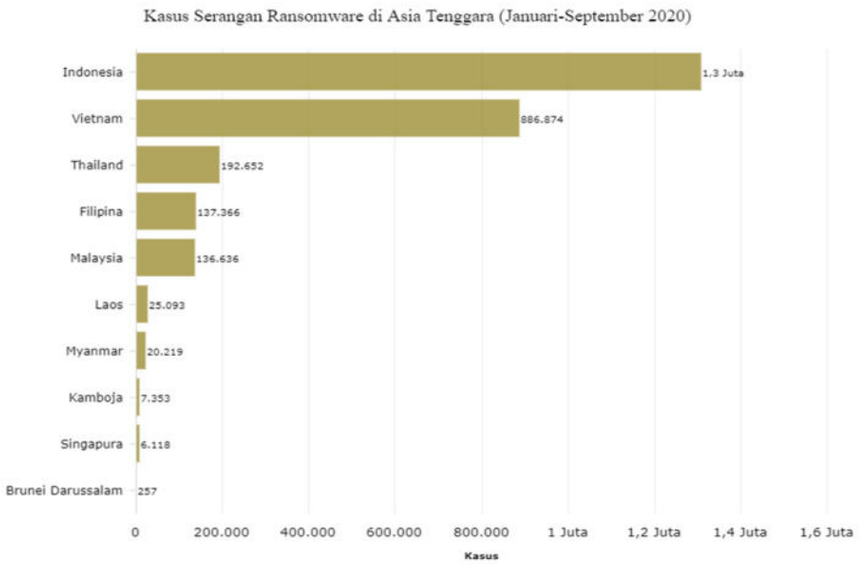
Menurut laporan 'Persepsi Publik atas Pelindungan Data Pribadi 2021' yang dilakukan Kementerian Komunikasi dan Informatika, hal yang paling banyak mereka alami adalah berkurangnya uang tabungan di rekening bank (44,1%) akibat kebocoran data. Disusul berkurangnya saldo di *e-wallet* (32,2%). Kerugian lain yang dirasakan responden yaitu seperti melakukan transfer atau pembelian karena dihubungi oleh orang ataupun perusahaan tertentu.

Dari sejumlah produk perbankan atau lembaga keuangan, responden menilai *e-wallet* dan rekening bank sebagai produk yang dianggap rentan

mengalami kebocoran data. Tercatat, 36.6% responden yang mengatakan kebocoran data di dompet digital dan 30,2% rekening bank.

International Business Machines Corporation atau IBM mencatat, rata-rata kerugian biaya yang diakibatkan pelanggaran data (data breach) di dunia mencapai US$4,24 juta pada Tahun 2021. Jumlah tersebut meningkat 9,84% dibandingkan Tahun sebelumnya yang sebesar US$3,86 juta. Melihat trennya, jumlah rata-rata biaya yang dikeluarkan dari pelanggaran data berfluktuatif cenderung meningkat dalam tujuh tahun terakhir. Walau demikian, rekor biaya kerugian terjadi pada tahun lalu. Industri kesehatan menjadi sektor yang paling banyak mengalami kerugian akibat kasus pelanggaran data. Rata-rata biaya yang harus dikeluarkan mencapai US$9,23 juta pada tahun lalu. Posisinya diikuti oleh industri keuangan dengan rata-rata kerugian akibat pelanggaran data sebesar US$5,72 juta. Lalu, pelanggaran data di sektor farmasi dan teknologi menghabiskan biaya masing-masing sebesar US$5,04 juta dan US$4,88 juta.

Ancaman lain yang perlu diwaspadai dari kelemahan pengamanan akses adalah serangan *ransomware*. *Ransomware* merupakan salah satu jenis *malicious software* (*malware*) yang menggunakan metode enkripsi dengan mengubah data menjadi kode yang tidak dapat dibaca oleh perangkat. Sehingga, menyebabkan pemilik data kehilangan kendali penuh atas data tersebut. Mengutip data dari *Interpol Cyber Assessment Report* 2021, ada sekitar 2,7 juta serangan *ransomware* yang terdeteksi di negara-negara Asia Tenggara pada periode Januari-September 2020. Dari jumlah itu, Indonesia berada di peringkat teratas dengan 1,3 juta kasus. Hal ini dapat dilihat pada data yang disajikan pada Grafik 1 berikut:



Grafik 1 Kasus Serangan *Ransomware* di Kawasan Asia Tenggara Tahun 2020

Selain data pada Grafik 1, pada Laporan Tahunan *Monitoring* Keamanan Siber Tahun 2021 yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), tercatat bahwa ran*somware* menduduki peringkat kedua di Indonesia sebagai serangan yang paling banyak dilaporkan pada Tahun 2021. Angka aduan ini mengalami peningkatan sebanyak 7 (tujuh) kali lipat yang sebelumnya 8 (delapan) aduan menjadi 56 (lima puluh enam) aduan. Karenanya, perlu adanya upaya pencegahan dari pemerintah guna meminimalkan risiko terjadinya *ransomware* di kemudian hari.

Hal lain yang perlu menjadi perhatian adalah amanah Presiden Joko Widodo yang menyatakan bahwa "Data ini adalah jenis kekayaan baru. Saat ini data adalah *new oil*, bahkan lebih berharga dari minyak. Data yang valid menjadi salah satu kunci pembangunan. Data yang valid sangat dibutuhkan untuk menyusun perencanaan, anggaran, kemudian membuat kebijakan, hingga mengeksekusi kebijakan tersebut demi hasil yang efektif." Validitas data merupakan salah satu layanan keamanan yang ditawarkan oleh kriptografi modern selain layanan keamanan lainnya. Mengingat manfaatnya tersebut, maka kriptografi secara langsung turut serta dalam menyukseskan pembangunan negara.

Merujuk pada berbagai data dan fakta di atas, maka dapat disimpulkan bahwa kriptografi merupakan bidang yang perlu

dikembangkan dan dioptimalkan pemanfaatannya di Indonesia. Guna mendorong berkembangnya pemanfaatan kriptografi di Indonesia, salah satu langkah penting yang perlu dilakukan adalah menyediakan Standar Kompetensi Kerja Nasional Indonesia (SKKNI) di bidang Kriptografi. Dengan adanya SKKNI ini, dapat menjadi rujukan bagi industri dalam negeri untuk mengembangkan produk kriptografi yang memenuhi aspek kerahasiaan, autentikasi, ketersediaan, keutuhan, akuntabilitas, dan otorisasi yang sesuai dengan kebutuhan pengguna.

Pengembangan produk kriptografi perlu diawali dengan analisis kebutuhan, guna memastikan kesesuaian antara tujuan pengembangan dengan solusi yang nantinya akan dibuat. Pada tahapan ini, sebaiknya juga dilakukan penelaahan terhadap tren teknologi, faktor-faktor risiko, serta regulasi dan standar apa saja yang terkait. Hasil dari analisis kebutuhan ini selanjutnya akan menjadi acuan dalam menentukan rincian dari desain produk kriptografi yang akan dikembangkan. Hal ini termasuk dengan perumusan spesifikasi teknis, membangun skema serta memastikan kekuatannya melalui analisis matematis. Tahapan ini sangat penting, karena suatu desain yang tidak dapat memenuhi kriteria analisis matematis artinya belum dapat menjawab kebutuhan keamanan yang diinginkan dan perlu diperbaiki kembali.

Tahapan selanjutnya adalah melakukan implementasi terhadap desain yang dibuat agar menjadi suatu produk kriptografi yang dapat digunakan. Pada tahap ini perlu diperhatikan pemilihan metode dan *platform* yang akan digunakan agar implementasi yang dilakukan sesuai dengan syarat yang telah ditentukan.

Langkah penting selanjutnya adalah melakukan pengujian terhadap produk kriptografi yang dilakukan. Langkah ini sangat penting sebagai upaya untuk mewujudkan *assurance* dari produk kriptografi yang dibuat. Ada berbagai metode pengujian yang dapat dilakukan sesuai dengan jenis algoritma yang digunakan, metode implementasi, *platform*, serta jenis serangan yang akan diujikan. Termasuk pada tahap ini adalah uji fungsi untuk memastikan apakah produk kriptografi berfungsi sebagaimana mestinya. Pada tahap ini diperlukan wawasan yang luas, objektivitas serta

ketelitian yang tinggi agar meminimalikan risiko terjadinya celah keamanan pada produk kriptografi yang dibuat.

Dalam mengembangkan kriptografi, terdapat beberapa standar yang perlu menjadi perhatian. Diantaranya adalah standar yang dikeluarkan oleh *American National Standards Institute* (ANSI) yang terkenal dengan beberapa seri ANSI X9 yang terkait dengan penerapan kriptografi. Selain itu, juga ada *International Telecommunications Union* (ITU-T) yang bertanggung jawab untuk standarisasi elemen-elemen seperti direktori X.400, X.500 serta sertifikat X.509. Dalam hal penerapan kriptografi kunci publik, juga perlu mengacu pada standar yang diterbitkan oleh *Public-Key Cryptographic Standards* (PKCS).

International Organization for Standardization (ISO) melalui *International Electrotechnical Commission* (IEC) menerbitkan beberapa standar ISO/IEC yang berkaitan dengan kriptografi. Beberapa diantaranya telah diadopsi sebagai Standar Nasional Indonesia (SNI), yakni SNI ISO/IEC 20085-2:2020, SNI ISO/IEC 20540:2018, SNI 8542:2018 ISO/IEC 24759:2017, SNI 8537:2018 ISO/IEC 17825:2016, dan SNI ISO/IEC 19790:2015.

Selain standar tersebut di atas, pada Tahun 2019, BSSN telah menerbitkan Peta Okupasi Nasional Keamanan Siber yang memuat 30 (tiga puluh) okupasi bidang keamanan siber. Di dalam peta okupasi tersebut, terdapat 4 (empat) okupasi di bidang kriptografi yang berhubungan erat dengan pengembangan produk kriptografi. Okupasi yang dimaksud adalah *Cryptography Specialist, Cryptography Engineer, Cryptography Module Analyst,* dan *Cryptography Analyst*. Seluruh okupasi tersebut telah dilengkapi deskripsinya, namun belum ada unit kompetensi yang dapat menjadi rujukan. Karenanya, penyusunan SKKNI Kriptografi merupakan suatu kebutuhan yang mutlak perlu dilakukan untuk menumbuhkan profesi bidang kriptografi.

Upaya dalam menumbuhkan industri kriptografi di Indonesia secara langsung selaras dengan upaya untuk menumbuhkan kemandirian teknologi di dalam negeri. Tentunya hal ini juga akan semakin memperkuat keamanan dan ketahanan siber secara nasional.

B. Pengertian

1. Kriptografi adalah suatu disiplin yang meliputi prinsip, sarana dan metode untuk transformasi data dalam rangka menyembunyikan kandungan semantik, mencegah penyalahgunaan wewenang, atau mencegah modifikasi tak terdeteksi.
2. Produk Kriptografi adalah perangkat lunak, perangkat keras, *firmware*, atau *hybrid* yang mencakup satu atau lebih fungsi kriptografi.
3. Algoritma Kriptografi merupakan prosedur komputasi yang terdefinisi dengan baik dan memiliki *input* variabel, termasuk kunci kriptografi dan menghasilkan luaran.
4. Batasan Kriptografi merupakan perimeter kontinu yang menetapkan batas fisik dan/atau *logic* dari produk kriptografi dan berisi semua komponen perangkat keras, perangkat lunak, dan/atau *firmware* produk kriptografi.
5. Aspek keamanan kriptografi meliputi kerahasiaan (*confidentiality*), keutuhan data (*integrity*), ketersediaan (*availability*), otorisasi (*authorization*), autentikasi (*authentication*), dan akuntabilitas (*accountability*).

C. Penggunaan SKKNI

Standar Kompetensi dibutuhkan oleh beberapa lembaga/institusi yang berkaitan dengan pengembangan sumber daya manusia, sesuai dengan kebutuhan masing-masing:

1. Untuk institusi pendidikan dan pelatihan
   a. Memberikan informasi untuk pengembangan program dan kurikulum.
   b. Sebagai acuan dalam penyelenggaraan pelatihan, penilaian, dan sertifikasi.
2. Untuk dunia usaha/industri dan penggunaan tenaga kerja
   a. Membantu dalam rekrutmen.
   b. Membantu penilaian unjuk kerja.

c. Membantu dalam menyusun uraian jabatan.

d. Membantu dalam mengembangkan program pelatihan yang spesifik berdasar kebutuhan dunia usaha/industri.

3. Untuk institusi penyelenggara pengujian dan sertifikasi

a. Sebagai acuan dalam merumuskan paket-paket skema sertifikasi sesuai dengan kualifikasi dan levelnya.

b. Sebagai acuan dalam penyelenggaraan pelatihan penilaian dan sertifikasi.

D. Komite Standar Kompetensi

Susunan komite standar kompetensi pada Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Bidang Kriptografi melalui keputusan Kepala Badan Siber dan Sandi Negara Nomor 198 Tahun 2022 tentang Pembentukan Komite, Tim Perumus, Tim Verifikasi, dan Sekretariat Penyusunan Standar Kompetensi Kerja Nasional Indonesia Bidang Kriptografi tanggal 12 Mei 2022 dapat dilihat pada Tabel 1, Tabel 2, dan Tabel 3.

Tabel 1. Susunan Komite Standar Kompetensi SKKNI Bidang Kriptografi

NO.	NAMA	INSTANSI/ LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Kepala Badan Siber dan Sandi Negara	Badan Siber dan Sandi Negara	Pengarah
2.	Wakil Kepala Badan Siber dan Sandi Negara	Badan Siber dan Sandi Negara	Penanggung Jawab
3.	Deputi Bidang Strategi dan Kebijakan	Badan Siber dan Sandi Negara	Ketua
4.	Direktur Kebijakan Sumber Daya Manusia Keamanan Siber dan Sandi	Badan Siber dan Sandi Negara	Wakil Ketua
5.	Koordinator Bidang Standarisasi Direktorat	Badan Siber dan	Sekretaris

NO.	NAMA	INSTANSI/ LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
	Kebijakan Sumber Daya Manusia Keamanan Siber dan Sandi	Sandi Negara	
6.	Kepala Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi	Badan Siber dan Sandi Negara	Anggota
7.	Direktur Kebijakan Teknologi Keamanan Siber dan Sandi	Badan Siber dan Sandi Negara	Anggota
8.	Direktur Politeknik Siber dan Sandi Negara	Politeknik Siber dan Sandi Negara	Anggota
9.	Ketua Indonesia Cyber Security Forum	Indonesia Cyber Security Forum (ICSF)	Anggota
10.	Ketua Bidang Keamanan Siber	Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)	Anggota

Tabel 2. Susunan Tim Perumus SKKNI Bidang Kriptografi

NO.	NAMA	INSTANSI/ LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Ir. Budi Rahardjo, M.Sc., Ph.D.	Institut Teknologi Bandung (ITB)	Pengarah
2.	Martianus Frederic Ezerman, Ph.D.	PT Sandhiguna Widya Proteksi	Ketua
3.	Dr. Bety Hayat Susanti, S.Si., M.E.	Politeknik Siber dan Sandi Negara	Sekretaris
4.	Risman Adnan, Ph.D.	Samsung R&D Indonesia	Anggota
5.	Gajendran Kandasamy, Ph.D.	PT Indonesia Digital Identity	Anggota
6.	Ir. Ari Moesriami Barmawi, M.Sc., Ph.D.	Universitas Telkom	Anggota
7.	Ir. Setiadi Yazid, M.Sc., Ph.D.	Universitas Indonesia	Anggota
8.	Dr. Sugi Guritman	Institut Pertanian Bogor	Anggota
9.	Satriyo Wibowo, S.T., MBA, M.H.	Indonesia Cyber Security Forum	Anggota
10.	Fakhmi Kemal Islamy, ST.	PT Telekomunikasi Selular	Anggota
11.	Muhammad Arief, MSEE., M.Sc.	Badan Riset dan Inovasi Nasional (BRIN)	Anggota
12.	Sari Agustini Hafman, S.Stat., M.Si.	Badan Siber dan Sandi Negara (BSSN)	Anggota
13.	Wildan, S.ST., M.Si	Badan Siber dan Sandi Negara (BSSN)	Anggota
14.	Sandromedo Christa Nugroho, S.ST., M.Han.	Asosiasi Fungsional Sandiman Indonesia	Anggota
15.	Muhammad Syahral, S.T., M.T.	Politeknik Siber dan Sandi Negara	Anggota
16.	Tetra Widianto, S.ST.	Badan Siber dan Sandi Negara (BSSN)	Anggota

Tabel 3. Susunan Tim Verifikasi SKKNI Bidang Kriptografi

NO.	NAMA	INSTANSI/ LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Anas Hilal, S.Pd.	Badan Siber dan Sandi Negara	Ketua
2.	Rian Irawan	Badan Siber dan Sandi Negara	Anggota
3.	Mita Pramihapsari, S.ST.MP	Badan Siber dan Sandi Negara	Anggota
4.	Roybafih Sukisman, S.Tr.TP	Badan Siber dan Sandi Negara	Anggota

BAB II
STANDAR KOMPETENSI KERJA NASIONAL INDONESIA

A. Pemetaan Standar Kompetensi

TUJUAN	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
Mengembangkan kriptografi untuk mencapai kerahasiaan, autentikasi, ketersediaan, keutuhan, akuntabilitas, dan otorisasi sesuai kebutuhan pengguna	Mengembangkan desain produk kriptografi	Menelaah produk kriptografi yang dibutuhkan	Menentukan kebutuhan keamanan minimal produk kriptografi
			Menentukan ruang lingkup produk kriptografi
		Menetapkan desain produk kriptografi yang dibutuhkan	Merumuskan spesifikasi desain produk kriptografi
			Membangun Skema Kriptografi
		Memastikan kekuatan matematis desain produk kriptografi	Menentukan Metode analisis matematis terhadap desain produk kriptografi
			Melakukan analisis matematis terhadap desain produk kriptografi
	Mengembangkan produk kriptografi	Merancang model implementasi desain produk kriptografi	Menentukan metode pemodelan yang relevan dengan kebutuhan desain produk kriptografi
			Melakukan integrasi fungsi kriptografi dan fungsi pendukungnya
		Menerapkan model implementasi menjadi produk kriptografi	Melakukan implementasi rancangan teknis produk kriptografi
			Melakukan dokumentasi implementasi

			desain produk kriptografi
			Menyusun panduan penggunaan produk kriptografi
	Mengembangkan pengujian produk kriptografi	Merancang pengujian terhadap implementasi desain	Menentukan metode pengujian yang akan dilakukan
			Menyusun skenario pengujian produk kriptografi
		Melakukan pengujian sesuai skenario pengujian	Melakukan pengujian terhadap produk kriptografi
			Menyusun rekomendasi berdasarkan hasil pengujian

B. Daftar Unit Kompetensi

NO.	KODE UNIT	JUDUL UNIT KOMPETENSI
1	*2*	*3*
1.	J.61KRP00.001.1	Menentukan Kebutuhan Keamanan Minimal Produk Kriptografi
2.	J.61KRP00.002.1	Menentukan Ruang Lingkup Produk Kriptografi
3.	J.61KRP00.003.1	Menetapkan Spesifikasi Desain Produk Kriptografi
4.	J.61KRP00.004.1	Membangun Skema Kriptografi
5.	J.61KRP00.005.1	Menentukan Metode Analisis Matematis Terhadap Desain Produk Kriptografi
6.	J.61KRP00.006.1	Melakukan Analisis Matematis Terhadap Desain Produk Kriptografi
7.	J.61KRP00.007.1	Menentukan Metode Pemodelan yang Relevan Dengan Kebutuhan Desain Produk Kriptografi
8.	J.61KRP00.008.1	Melakukan Integrasi Fungsi Kriptografi dan Fungsi Pendukungnya
9.	J.61KRP00.009.1	Melakukan Implementasi Rancangan Teknis Produk Kriptografi
10.	J.61KRP00.010.1	Melakukan Dokumentasi Implementasi Desain Produk Kriptografi
11.	J.61KRP00.011.1	Menyusun Panduan Penggunaan Produk Kriptografi
12.	J.61KRP00.012.1	Menentukan Metode Pengujian yang akan Dilakukan
13.	J.61KRP00.013.1	Menyusun Skenario Pengujian Produk Kriptografi
14.	J.61KRP00.014.1	Melakukan Pengujian Terhadap Produk Kriptografi
15.	J.61KRP00.015.1	Menyusun Rekomendasi Berdasarkan Hasil Pengujian

C. Uraian Unit Kompetensi

KODE UNIT : **J.61KRP00.001.1**

JUDUL UNIT : **Menentukan Kebutuhan Keamanan Minimal Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menentukan kebutuhan keamanan minimal produk kriptografi melalui pengidentifikasian dan perumusan kebutuhan keamanan minimal produk kriptografi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi kebutuhan keamanan minimal produk kriptografi	1.1 Informasi terkait **sistem elektronik** diinventarisasi berdasarkan ruang lingkup layanan, jenis aset yang dikelola, klasifikasi informasi, **risiko**, dan proses bisnis sistem elektronik. 1.2 **Informasi kerawanan** diinventarisasi berdasarkan tren serangan terkait. 1.3 Ketentuan pengamanan sistem elektronik ditelaah berdasarkan kebijakan terkait. 1.4 Kebutuhan keamanan sistem elektronik ditelaah berdasarkan risiko, informasi kerawanan maupun kebijakan terkait. 1.5 Kebutuhan aspek keamanan sistem elektronik ditentukan berdasarkan hasil telaah kebutuhan keamanan sistem elektronik.
2. Merumuskan kebutuhan keamanan minimal produk kriptografi	2.1 **Referensi** terkait produk kriptografi dikumpulkan berdasarkan aspek keamanan terkait. 2.2 **Kebutuhan keamanan minimal produk kriptografi** dianalisis berdasarkan hasil telaah kebijakan, standar dan *best practice* terkait. 2.3 Kebutuhan keamanan minimal produk kriptografi disusun berdasarkan hasil telaah terkait.

BATASAN VARIABEL

1. Konteks variabel

1.1 Unit kompetensi ini berlaku untuk mengidentifikasi dan merumuskan kebutuhan keamanan minimal produk kriptografi.

1.2 Sistem elektronik yang dimaksud merupakan serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronic Data Interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

1.3 Risiko yang dimaksud berupa informasi terkait kerentanan yang diperoleh melalui kegiatan penilaian risiko maupun kegiatan pengembangan produk kriptografi yang dilakukan terhadap sistem elektronik dan berdasarkan pendekatan lainnya.

1.4 Informasi kerawanan yang dimaksud dapat berupa informasi terkait dengan serangan yang sedang berkembang saat ini terhadap sistem elektronik serupa, tren insiden yang terjadi terhadap sistem elektronik serupa, serangan dan insiden yang secara teoritis dapat terjadi pada sistem elektronik serupa atau serangan dan insiden yang terjadi pada lingkup sistem elektronik terkait, dan/atau informasi kerawanan lainnya.

1.5 Referensi yang dimaksud dapat berupa standar, dokumen *best practice*, maupun hasil kajian yang relevan dengan kebutuhan dalam pengembangan produk kriptografi.

1.6 Kebutuhan keamanan minimal produk kriptografi berupa informasi terkait kekuatan keamanan minimal yang harus dipenuhi berdasarkan standar maupun *best practice* yang dipilih menjadi rujukan dalam penerapan dan pemilihan algoritma kriptografi, manajemen kunci, penerapan *encryption at rest,*

encryption in use, dan *encryption in transit*. Misalnya, standar keamanan yang harus dipenuhi pada perbankan dengan menggunakan sistem *Open Application Programming Interface* (API) adalah autentikasi sesuai rancangan bank/*fintech* (*Two Factor Authentication* (2FA)), otorisasi: *Open Authorization* (O.Auth) 2.0 dan enkripsi: SHA-2/AES-256. Karenanya, kebutuhan keamanan minimal yang ditentukan tidak boleh lebih rendah dari ketentuan tersebut.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001 Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan
      4.2.2 SNI ISO/IEC 27002 Teknologi informasi – Teknik keamanan – Panduan praktik kendali keamanan informasi

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

1.4 Hasil unjuk kerja berupa hasil telaah kebutuhan keamanan sistem elektronik dan kebutuhan keamanan minimal produk kriptografi.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Keamanan sistem elektronik

3.1.2 Ruang lingkup produk kriptografi

3.2 Keterampilan

3.2.1 Menyusun laporan secara sistematis

4. Sikap kerja yang diperlukan

4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi

4.2 Teliti dalam menelaah kebutuhan keamanan sistem elektronik

4.3 Obyektif dalam menentukan kebutuhan keamanan minimal produk kriptografi

4.4 Bertanggung jawab dalam menentukan kebutuhan keamanan minimal produk kriptografi

5. Aspek kritis

5.1 Ketepatan dalam menyusun kebutuhan keamanan minimal produk kriptografi berdasarkan hasil telaah terkait

KODE UNIT : **J.61KRP00.002.1**

JUDUL UNIT : **Menentukan Ruang Lingkup Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menentukan ruang lingkup produk kriptografi melalui penelaahan referensi dan penyusunan ruang lingkup produk kriptografi yang akan dikembangkan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menelaah referensi terkait produk kriptografi	1.1 **Referensi** diidentifikasi berdasarkan relevansinya dengan kebutuhan produk kriptografi. 1.2 Referensi dianalisis berdasarkan kebutuhan keamanan minimal produk kriptografi. 1.3 Hasil analisis disusun berdasarkan kebutuhan aspek keamanan kriptografi.
2. Menyusun ruang lingkup produk kriptografi	2.1 Data terkait **ruang lingkup produk kriptografi** dikumpulkan berdasarkan hasil analisis. 2.2 Rincian ruang lingkup produk kriptografi dikonfirmasikan kepada pemangku kepentingan berdasarkan kewenangannya. 2.3 Ruang lingkup produk kriptografi dirumuskan sesuai hasil konfirmasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menelaah referensi dan menyusun ruang lingkup produk kriptografi.
   1.2 Referensi yang dimaksud dapat berupa standar, dokumen *best practice*, maupun hasil kajian yang relevan dengan kebutuhan dalam pengembangan produk kriptografi.
   1.3 Ruang lingkup produk kriptografi yang dimaksud paling sedikit memuat informasi yang terkait tujuan penyediaan produk kriptografi, fungsi kriptografi yang dibutuhkan, aspek keamanan yang disasar, kebutuhan keamanan minimal, cakupan

penggunaan dan tipe produk kriptografi yang dibutuhkan (perangkat keras, perangkat lunak, *firmware,* atau *hybrid*). Apabila diperlukan, ruang lingkup yang dimaksud dapat memuat informasi terkait proses bisnis produk kriptografi yang akan dikembangkan, manfaat yang akan diterima oleh organisasi, unit penanggung jawab dan penggunanya maupun komponen lain yang dianggap perlu oleh organisasi.

2. Peralatan dan perlengkapan
   - 2.1 Peralatan
     - 2.1.1 Komputer dan/atau perangkat pengolahan data
     - 2.1.2 Internet
   - 2.2 Perlengkapan
     - 2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

   (Tidak ada.)

4. Norma dan standar
   - 4.1 Norma

     (Tidak ada.)
   - 4.2 Standar
     - 4.2.1 NIST SP 800-175B Rev. 1 *Guideline for Using Cryptographic Standards in the Federal Government*: Cryptographic *Mechanisms*
     - 4.2.2 SNI ISO/IEC 19790:2015 Teknik keamanan – Persyaratan keamanan untuk modul kriptografi
     - 4.2.3 SNI ISO/IEC 18033-1: 2021 Keamanan informasi – Algoritma enkripsi – Bagian 1: Umum
     - 4.2.4 SNI ISO/IEC 18033-2: 2006 Teknologi informasi – Teknik keamanan - Algoritma enkripsi – Bagian 2: Penyandian asimetris.

4.2.5 SNI ISO/IEC 18033-3: 2010 Teknologi informasi – Teknik keamanan - Algoritma enkripsi – Bagian 3: Penyandian blok

4.2.6 SNI ISO/IEC 18033-4: 2011 Teknologi informasi – Teknik keamanan - Algoritma enkripsi – Bagian 4: Penyandian alir

4.2.7 SNI ISO/IEC 18033-5: 2015 Teknologi informasi – Teknik keamanan – Algoritma enkripsi – Bagian 5: Penyandian berbasis identitas

4.2.8 SNI ISO/IEC 18033-6: 2019 Teknik keamanan teknologi informasi - Algoritma enkripsi – Bagian 6: Enkripsi *homomorphic*

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

   1.4 Hasil unjuk kerja berupa dokumen analisis kebutuhan dan rumusan ruang lingkup produk kriptografi.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
    3.1 Pengetahuan
        3.1.1 Prinsip-prinsip keamanan kriptografi
        3.1.2 Jenis produk kriptografi
    3.2 Keterampilan
        3.2.1 Mengoperasikan perangkat keras dan perangkat lunak
        3.2.2 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami terkait ruang lingkup produk kriptografi

4. Sikap kerja yang diperlukan
    4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi
    4.2 Teliti dalam mengumpulkan informasi
    4.3 Objektif dalam menentukan kebutuhan kriptografi
    4.4 Bertanggung jawab dalam menentukan ruang lingkup produk kriptografi yang akan dikembangkan oleh organisasi

5. Aspek kritis
    5.1 Ketepatan dalam merumuskan ruang lingkup produk kriptografi berdasarkan hasil konfirmasi

KODE UNIT : **J.61KRP00.003.1**

JUDUL UNIT : **Menetapkan Spesifikasi Desain Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menetapkan spesifikasi desain produk kriptografi melalui penelaahan dan penentuan spesifikasi desain produk kriptografi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menelaah ruang lingkup produk kriptografi	1.1 **Informasi** dikumpulkan berdasarkan rincian pada **ruang lingkup produk kriptografi**. 1.2 Algoritma dan modul kriptografi dianalisis berdasarkan kesesuaiannya dengan ruang lingkup produk kriptografi.
2. Menentukan spesifikasi desain produk kriptografi	2.1 Daftar algoritma dan modul kriptografi disusun berdasarkan ruang lingkup produk kriptografi. 2.2 Spesifikasi desain produk kriptografi dirumuskan berdasarkan daftar algoritma dan modul kriptografi yang sesuai.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menelaah ruang lingkup produk kriptografi dan menentukan spesifikasi desain produk kriptografi.
   1.2 Informasi yang dimaksud meliputi kebijakan/standar/*best practice* yang terkait dengan rincian pada ruang lingkup produk kriptografi serta informasi faktual terkait tren di bidang kriptografi itu sendiri.
   1.3 Ruang lingkup produk kriptografi yang dimaksud paling sedikit memuat informasi yang terkait tujuan penyediaan produk kriptografi, fungsi kriptografi yang dibutuhkan, aspek keamanan yang disasar, kebutuhan keamanan minimal, cakupan

penggunaan dan tipe produk kriptografi yang dibutuhkan (*hardware, software, firmware,* atau *hybrid*).

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Peralatan yang terhubung ke jaringan internet
      2.1.3 Internet
   2.2 Perlengkapan
      2.2.1 Dokumen ruang lingkup produk kriptografi

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      4.2.1 NIST SP 800-175B Rev. 1 *Guideline for Using Cryptographic Standards in the Federal Government*: Cryptographic *Mechanisms*
      4.2.2 SNI ISO/IEC 19790:2015 Teknologi informasi – Teknik keamanan – Persyaratan keamanan untuk modul kriptografi
      4.2.3 SNI ISO/IEC 18033-1: 2021 Keamanan informasi – Algoritma enkripsi – Bagian 1: Umum
      4.2.4 SNI ISO/IEC 18033-2: 2006 Teknologi informasi – Teknik keamanan - Algoritma enkripsi – Bagian 2: Penyandian asimetris.
      4.2.5 SNI ISO/IEC 18033-3: 2010 Teknologi informasi – Teknik keamanan - Algoritma enkripsi – Bagian 3: Penyandian blok
      4.2.6 SNI ISO/IEC 18033-4: 2011 Teknologi informasi – Teknik keamanan - Algoritma enkripsi – Bagian 4: Penyandian alir

4.2.7 SNI ISO/IEC 18033-5: 2015 Teknologi informasi – Teknik keamanan – Algoritma enkripsi – Bagian 5: Penyandian berbasis identitas

4.2.8 SNI ISO/IEC 18033-6: 2019 Teknik keamanan teknologi informasi - Algoritma enkripsi – Bagian 6: Enkripsi *homomorphic*

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

   1.4 Hasil unjuk kerja berupa daftar algoritma dan modul kriptografi pada rincian spesifikasi desain produk kriptografi.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

   3.1 Pengetahuan

      3.1.1 Algoritma kriptografi

      3.1.2 Protokol kriptografi

      3.1.3 Manajemen kunci kriptografi

      3.1.4 Analisis kompleksitas algoritma

3.2 Keterampilan

3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami terkait spesifikasi desain produk kriptografi

4. Sikap kerja yang diperlukan

4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi

4.2 Obyektif dalam menentukan algoritma dan modul kriptografi yang sesuai kebutuhan

4.3 Teliti dalam menetapkan spesifikasi desain produk kriptografi

4.4 Bertanggung jawab terhadap penetapan spesifikasi desain produk kriptografi

5. Aspek kritis

5.1 Ketepatan dalam merumuskan spesifikasi desain produk kriptografi sesuai daftar algoritma dan modul kriptografi yang sesuai

KODE UNIT : **J.61KRP00.004.1**

JUDUL UNIT : **Membangun Skema Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam membangun skema kriptografi melalui penentuan algoritma kriptografi dan penyusunan desain produk kriptografi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan algoritma kriptografi yang sesuai	1.1 **Algoritma kriptografi** diinventarisasi berdasarkan spesifikasi produk kriptografi. 1.2 Algoritma kriptografi dipilih berdasarkan kesesuaian dengan spesifikasi desain produk kriptografi.
2. Menyusun desain produk kriptografi	2.1 **Skema kriptografi** dirumuskan sesuai spesifikasi desain produk kriptografi. 2.2 Skema kriptografi divalidasi kesesuaiannya dengan spesifikasi desain produk kriptografi. 2.3 Desain produk kriptografi dirumuskan berdasarkan integrasi skema kriptografi yang sesuai.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan algoritma dan menyusun desain produk kriptografi.
   1.2 Algoritma kriptografi merupakan prosedur komputasi yang terdefinisi dengan baik dan memiliki input variabel, termasuk kunci kriptografi dan menghasilkan luaran.
   1.3 Skema kriptografi berisi urutan algoritma kriptografi beserta spesifikasi parameter yang digunakan. Misalnya pada skema enkripsi dapat dipilih skema enkripsi dengan kunci simetris atau dengan kunci asimetris.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)
      2.2.2 Dokumen ruang lingkup produk kriptografi
      2.2.3 Dokumen spesifikasi desain produk kriptografi

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      4.2.1 NIST SP 800-175B *Rev. 1 Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*
      4.2.2 SNI ISO/IEC 19790:2015 Teknologi informasi – Teknik keamanan – Persyaratan keamanan untuk modul kriptografi
      4.2.3 NIST SP 800-130 *A Framework for Designing Cryptographic Key Management Systems*

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan

peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

1.4 Hasil unjuk kerja berupa skema kriptografi yang telah tervalidasi kesesuaiannya dengan spesifikasi produk yang telah ditetapkan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Rekayasa komputer

3.1.2 Algoritma kriptografi

3.1.3 Protokol kriptografi

3.1.4 Manajemen kunci kriptografi

3.2 Keterampilan

3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menjabarkan skema produk kriptografi

4. Sikap kerja yang diperlukan

4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi

4.2 Teliti dalam menginventarisasi algoritma kriptografi yang sesuai

5. Aspek kritis

5.1 Ketepatan dalam merumuskan desain produk kriptografi berdasarkan integrasi skema kriptografi yang sesuai

KODE UNIT : **J.61KRP00.005.1**

JUDUL UNIT : **Menentukan Metode Analisis Matematis Terhadap Desain Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menentukan metode analisis matematis terhadap desain produk kriptografi melalui penelaahan algoritma, penyusunan daftar model serangan, dan penetapan metode analisis matematis terhadap desain produk kriptografi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menelaah algoritma desain produk kriptografi	1.1 **Referensi** diidentifikasi berdasarkan relevansinya dengan karakteristik algoritma. 1.2 **Kemungkinan kelemahan algoritma** dianalisis berdasarkan hasil identifikasi pada referensi.
2. Menyusun daftar model serangan	2.1 Referensi diidentifikasi berdasarkan relevansinya dengan desain produk kriptografi. 2.2 Model **serangan** diinventarisasi sesuai dengan hasil identifikasi referensi.
3. Menetapkan metode analisis matematis	3.1 **Metode analisis matematis** diinventarisasi sesuai dengan inventarisasi model serangan. 3.2 Metode analisis matematis ditentukan sesuai model serangan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menelaah algoritma, menyusun daftar model serangan, dan menetapkan metode analisis matematis terhadap desain produk kriptografi.
   1.2 Referensi yang dimaksud meliputi hasil kajian maupun publikasi yang memuat informasi terkait kelemahan matematis pada suatu algoritma kriptografi serta model serangan matematis dan metode

analisis matematis yang dapat dilakukan terhadap suatu algoritma kriptografi.

1.3 Kemungkinan kelemahan algoritma yang dimaksud dapat meliputi kelemahan terkait pendekatan matematis yang digunakan, jumlah *round*, skema/alur di dalam algoritma, kelemahan pada *block diagram* dan sebagainya yang telah dibuktikan dalam penelitian atau kajian terdahulu.

1.4 Model serangan meliputi algoritma serangan dan *platform* implementasi serangan dengan pendekatan matematis. Model serangan ditentukan berdasarkan karakteristik dan jenis algoritma kriptografi yang akan digunakan. Contohnya adalah serangan *Greatest Common Divisor* (GCD) yang dapat diterapkan pada algoritma Rivest Shamir Adleman (RSA). *Differential cryptanalysis* dan *linear cryptanalysis, truncated differentials, the square attacks* dan *interpolation attacks* yang dapat diterapkan untuk algoritma simetris.

1.5 Metode analisis matematis ditentukan berdasarkan algoritma serangan dan *platform*, meliputi analisis kompleksitas waktu dan memori.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 Internet

2.2 Perlengkapan

2.2.1 Kertas kerja

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 NIST SP 800-130 *Framework for Designing Cryptographic Key Management System*

4.2.2 NIST SP 800-57 *Part 1, Part 2, Part 3 Key Management Guidelines*

4.2.3 NIST SP 800-131A *Rev.2 Transitioning the Use of Cryptographic Algorithms and Key Lengths*

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

1.4 Hasil unjuk kerja berupa hasil telaah metode analisis matematis terhadap desain produk kriptografi.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Matematika kriptografi

3.1.2 Analisis kompleksitas algoritma

3.1.3 Model serangan matematis

3.2 Keterampilan

3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menjabarkan metode analisis matematis produk kriptografi

4. Sikap kerja yang diperlukan

4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi

4.2 Teliti dalam menemukan kemungkinan kelemahan algoritma kriptografi melalui pendekatan matematis

4.3 Bertanggung jawab terhadap pemilihan metode analisis keamanan

5. Aspek kritis

5.1 Ketepatan dalam memilih metode analisis matematis sesuai model serangan

KODE UNIT : **J.61KRP00.006.1**

JUDUL UNIT : **Melakukan Analisis Matematis terhadap Desain Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam dalam melakukan analisis matematis terhadap desain kriptografi melalui pengidentifikasian kriteria analisis matematis dan penelaahan nilai kompleksitas serangan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi kriteria analisis matematis	1.1 **Kriteria analisis matematis** diinventarisasi sesuai metode analisis matematis yang terpilih. 1.2 Kriteria analisis matematis ditentukan sesuai penetapan level keamanan.
2. Menelaah nilai kompleksitas serangan	2.1 **Nilai kompleksitas** dari serangan dihitung berdasarkan penggunaan waktu dan memori. 2.2 Nilai kompleksitas dari serangan dianalisis berdasarkan perbandingannya dengan level keamanan. 2.3 Kekuatan matematis desain produk kriptografi ditentukan berdasarkan hasil analisis.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan kriteria analisis matematis dan mnelaah nilai kompleksitas serangan.
   1.2 Kriteria analisis matematis merupakan prinsip atau standar yang menjadi dasar tata cara menghitung kecepatan dan kebutuhan memori sebuah serangan.
   1.3 Nilai kompleksitas meliputi sumber daya waktu dan memori yang dibutuhkan penyerang untuk melakukan serangan secara efektif terhadap skema.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Kertas kerja

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.
   1.4 Hasil unjuk kerja berupa laporan hasil pengujian keamanan berbasis matematis terhadap desain kriptografi

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

   3.1 Pengetahuan

      3.1.1 Analisis kompleksitas algoritma

      3.1.2 Metode analisis matematis

   3.2 Keterampilan

      3.2.1 Menggunakan bahasa pemrograman untuk memudahkan analisis matematis

      3.2.2 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami dalam menjabarkan hasil analisis matematis yang dilakukan

4. Sikap kerja yang diperlukan

   4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi

   4.2 Teliti dalam melakukan pengujian keamanan berbasis matematis terhadap desain kriptografi

   4.3 Berpikir sistematis dan terstruktur dalam melakukan pengujian keamanan berbasis matematis terhadap desain kriptografi

5. Aspek kritis

   5.1 Ketepatan dalam menghitung nilai kompleksitas dari serangan berdasarkan waktu dan memori yang digunakan

KODE UNIT : **J.61KRP00.007.1**

JUDUL UNIT : **Menentukan Metode Pemodelan yang Relevan dengan Kebutuhan Desain Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menentukan metode pemodelan yang relevan dengan kebutuhan desain produk kriptografi melalui identifikasi aktivitas proses, identifikasi dan penyeleksian metode pemodelan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menguraikan aktivitas proses	1.1 **Aktivitas proses** diidentifikasi berdasarkan **kompleksitas desain produk kriptografi**. 1.2 Kebutuhan **sumber daya** diidentifikasi berdasarkan setiap jenis sumber daya yang tersedia. 1.3 Jangka waktu penyelesaian ditentukan berdasarkan kebutuhan alokasi waktu. 1.4 Rincian aktivitas proses disusun berdasarkan kompleksitas, sumber daya dan jangka waktu penyelesaian.
2. Mengidentifikasi metode pemodelan	2.1 **Kriteria pemilihan metode pemodelan** disusun sesuai karakteristik metode pemodelan. 2.2 Metode pemodelan dianalisis relevansinya terhadap kebutuhan desain produk kriptografi sesuai kriteria pemilihan pemodelan.
3. Menyeleksi metode pemodelan	3.1 **Tingkat relevansi** ditelaah berdasarkan hasil analisis relevansi. 3.2 Metode pemodelan dipilih berdasarkan analisis tingkat relevansinya.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengidentifikasi aktivitas proses, mengidentifikasi dan menyeleksi metode pemodelan.

1.2 Aktivitas proses yang dimaksud dalam model terstruktur mengidentifikasi serangkaian aktivitas yang diperlukan sesuai dengan lingkup desain produk kriptografi.

1.3 Kompleksitas desain produk kriptografi yang dimaksud adalah informasi lebih rinci yang memuat aspek teknis yang dibutuhkan pada desain berdasarkan algoritma, modul maupun skema yang dipilih.

1.4 Sumber daya yang dimaksud meliputi kemampuan komputasi, ketersediaan sumber daya manusia, dukungan anggaran, dan aspek materil lainnya.

1.5 Kriteria pemilihan metode pemodelan terdiri atas:

1.5.1 Kriteria prioritas pemilihan metode sesuai dengan sumber daya yang tersedia.

1.5.2 Kriteria keberlangsungan pengembangan produk sesuai kebutuhan. Keberlangsungan pengembangan produk yang dimaksud berkaitan dengan karakteristik dan rencana pengembangan produk apakah akan ditetapkan sebagai produk yang berkembang dalam berbagai versi atau sebagai produk yang dibuat secara spesifik untuk *service* maupun sasaran tertentu saja.

1.5.3 Kriteria kompleksitas metode pemodelan sesuai aktivitas proses.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 Internet

2.2 Perlengkapan

2.2.1 Alat Tulis Kantor (ATK)

2.2.2 Dokumen spesifikasi teknis desain produk kriptografi

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

(Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

1.4 Hasil unjuk kerja berupa hasil analisis relevansi metode pemodelan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Proses pembuatan produk kriptografi

3.1.2 Metode pemodelan

3.2 Keterampilan

3.2.1 Mampu menguraikan rincian yang diperlukan pada desain produk kriptografi

4. Sikap kerja yang diperlukan
    4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi
    4.2 Teliti dan cermat dalam menelaah metode pemodelan yang paling dibutuhkan
    4.3 Bertanggung jawab terhadap metode pemodelan yang dipilih

5. Aspek kritis
    5.1 Ketepatan dalam memilih metode pemodelan berdasarkan analisis tingkat relevansinya

KODE UNIT : **J.61KRP00.008.1**

JUDUL UNIT : **Melakukan Integrasi Fungsi Kriptografi dan Fungsi Pendukungnya**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan integrasi fungsi kriptografi dan fungsi pendukungnya melalui pengidentifikasian serta pelaksanaan tahapaan integrasi fungsi kriptografi dan fungsi pendukungnya.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyusun daftar fungsi kriptografi dan pendukungnya	1.1 **Komponen fungsi kriptografi dan pendukungnya** diidentifikasi sesuai dengan pemodelan produk kriptografi. 1.2 **Metode integrasi** ditentukan sesuai hasil identifikasi komponen fungsi kriptografi dan pendukungnya.
2. Melaksanakan tahapan integrasi fungsi kriptografi dan pendukungnya	2.1 Tahapan integrasi fungsi ditentukan berdasarkan metode integrasi. 2.2 Integrasi fungsi kriptografi dan fungsi pendukungnya diterapkan sesuai tahapan. 2.3 Hasil integrasi divalidasi berdasarkan proses implementasi. 2.4 **Format dan sistematika integrasi** diidentifikasi sesuai dengan kebutuhan. 2.5 **Dokumen hasil integrasi** disusun sesuai dengan format dan sistematika.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengidentifikasi fungsi, melakukan tahapan integrasi fungsi kriptografi dan pendukungnya.
   1.2 Komponen fungsi kriptografi dan pendukungnya yang dimaksud terdiri atas komponen fungsi kriptografi dan komponen fungsi pendukung dengan contoh sebagai berikut:

1.2.1 komponen fungsi kriptografi diantaranya meliputi: *substitution box* (*sbox*), *permutation box* (*pbox*), *add round key, key expansion* dan lain-lain.

1.2.2 Komponen fungsi pendukung diantaranya meliputi: *user interface* (antarmuka pengguna), *storage* (penyimpanan), *peripheral* (antarmuka perangkat), dan lain-lain.

1.3 Metode integrasi adalah cara atau teknik yang digunakan dalam mengintegrasikan komponen fungsi kriptografi dan pendukungnya.

1.4 Format dan sistematika integrasi adalah susunan, urutan, klasifikasi, dan pengelompokkan tertentu yang digunakan dalam penyusunan dokumen hasil integrasi.

1.5 Dokumen hasil integrasi adalah informasi terdokumentasi dalam bentuk diagram yang menggambarkan proses integrasi fungsi kriptografi dan pendukungnya. Pada dokumen ini juga memuat hasil temuan, permasalahan (termasuk jika ditemukan adanya *bug*), beserta rekomendasi untuk evaluasi desain produk kriptografi.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 Internet

2.2 Perlengkapan

2.2.1 Alat Tulis Kantor (ATK)

2.2.2 Format dan sistematika penyusunan integrasi fungsi kriptografi dan pendukungnya

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

(Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.
   1.4 Hasil unjuk kerja berupa dokumen hasil integrasi yang disusun sesuai format secara sistematis.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Metode integrasi fungsi
      3.1.2 Data Flow Diagram (DFD)
   3.2 Keterampilan
      3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai integrasi fungsi kriptografi dan fungsi pendukung

4. Sikap kerja yang diperlukan
    4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi
    4.2 Teliti menelaah komponen fungsi kriptografi dan pendukungnya
    4.3 Bertanggung jawab terhadap pengembangan produk kriptografi yang dilakukan

5. Aspek kritis
    5.1 Ketepatan dalam menerapkan integrasi fungsi kriptografi dan pendukungnya sesuai tahapan

KODE UNIT : **J.61KRP00.009.1**

JUDUL UNIT : **Melakukan Implementasi Rancangan Teknis Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan implementasi rancangan teknis produk kriptografi melalui perumusan dan penerapan *flowchart/pseudocode* serta penyusunan rekomendasi implementasi produk kriptografi

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Merumuskan *flowchart/pseudocode*	1.1 **Format dan sistematika *flowchart/pseudocode*** diidentifikasi sesuai kebutuhan. 1.2 Rangkaian proses ditelaah berdasarkan desain produk kriptografi. 1.3 ***Flowchart/pseudocode*** disusun berdasarkan alur sesuai format dan sistematika.
2. Menerapkan *flowchart/pseudocode*	2.1 Perangkat dan peralatan diidentifikasi sesuai dengan kebutuhan. 2.2 *Flowchart/pseudocode* diimplementasikan pada perangkat dan peralatan sesuai dengan hasil identifikasi. 2.3 ***Unit testing*** dilakukan sesuai hasil implementasi. 2.4 ***Integration testing*** dilakukan sesuai hasil implementasi.
3. Menyusun rekomendasi implementasi produk kriptografi	3.1 Implementasi *flowchart/pseudocode* dianalisis berdasarkan hasil *unit testing* dan *integration testing*. 3.2 Rekomendasi implementasi produk kriptografi dirumuskan berdasarkan hasil analisis.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menyusun dan menerapkan *flowchart/pseudocode* serta menyusun rekomendasi implementasi produk kriptografi.
   1.2 Format dan sistematika *flowchart/pseudocode* adalah susunan, urutan, klasifikasi dan pengelompokkan tertentu yang digunakan dalam penyusunan implementasi rancangan teknis produk kriptografi.
   1.3 *Flowchart/pseudocode* adalah bagan alur yang menampilkan langkah-langkah dan keputusan untuk menggambarkan sebuah proses dari suatu program dalam bentuk diagram dan dihubungkan dengan garis atau arah panah.
   1.4 *Unit testing* adalah proses pengujian hasil implementasi komponen-komponen penyusun produk kriptografi.
   1.5 *Integration testing* adalah proses pengujian hasil implementasi produk kriptografi secara keseluruhan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 *Development tools* dan *supporting libraries*
      2.1.3 Internet
   2.2 Perlengkapan
      2.2.1 Dokumen acuan rekomendasi perbaikan
      2.2.2 Format dan sistematika *flowchart/pseudocode*

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)

4.2 Standar

(Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.
   1.4 Hasil unjuk kerja berupa hasil implementasi *flowchart/pseudocode* dan dokumen rekomendasi implementasi produk kriptografi.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 *Data Flow Diagram* (DFD)
      3.1.2 Struktur data dan algoritma pemrograman
      3.1.3 Algoritma kriptografi
   3.2 Keterampilan
      3.2.1 Membaca dan mendeskripsikan *flowchart/pseudocode*
      3.2.2 Melakukan pemrograman
      3.2.3 Menggunakan *tools* dalam rangka *unit testing* dan *integration testing*

4. Sikap kerja yang diperlukan
    4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi
    4.2 Teliti dalam mengimplementasikan *flowchart/pseudocode* dan menguji hasil implementasi
    4.3 Bertanggung jawab terhadap rekomendasi implementasi produk kriptografi yang disusun

5. Aspek kritis
    5.1 Ketepatan dalam menyusun *flowchart/pseudocode* berdasarkan alur sesuai format dan sistematika
    5.2 Ketepatan dalam merumuskan rekomendasi implementasi produk kriptografi berdasarkan hasil analisis

KODE UNIT : **J.61KRP00.010.1**

JUDUL UNIT : **Melakukan Dokumentasi Implementasi Desain Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan dokumentasi implementasi desain produk kriptografi melalui penyiapan format dan perumusan dokumentasi implementasi produk kriptografi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyiapkan format dokumentasi	1.1 **Sumber data** diidentifikasi sesuai dengan hasil pemodelan, integrasi fungsi kriptografi dan pendukungnya, serta implementasi rancangan teknis produk kriptografi. 1.2 **Format dan sistematika dokumentasi** diidentifikasi sesuai dengan kebutuhan.
2. Merumuskan dokumentasi implementasi produk kriptografi	2.1. **Dokumentasi implementasi produk kriptografi** disusun sesuai dengan format dan sistematika. 2.2. **Pengesahan dokumentasi implementasi produk kriptografi** dilakukan sesuai dengan kebutuhan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menyiapkan format dan merumuskan dokumentasi implementasi produk kriptografi.
   1.2 Sumber data adalah sistem, proses, aktivitas, prosedur, atau objek lainnya yang menjadi asal dalam perolehan dokumentasi implementasi produk kriptografi.
   1.3 Format dan sistematika dokumentasi adalah susunan, urutan, klasifikasi, dan pengelompokkan tertentu yang digunakan dalam penyusunan dokumentasi implementasi produk kriptografi.
   1.4 Dokumentasi implementasi produk kriptografi adalah hasil dari penyusunan sumber data terhadap format dan sistematika untuk

menjelaskan dan menggambarkan implementasi produk kriptografi.

1.5 Pengesahan dokumentasi implementasi produk kriptografi meliputi proses reviu kesesuaian terhadap format dan sistematika serta penandatanganan hasil penyusunan dokumentasi implementasi produk kriptografi oleh pembuat laporan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)
      2.2.2 Format dan sistematika dokumentasi implementasi produk kriptografi

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan

peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

1.4 Hasil unjuk kerja berupa dokumentasi implementasi produk kriptografi sesuai format secara sistematis.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Produk kriptografi

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Menyusun narasi yang empiris dan mudah dipahami mengenai produk kriptografi

4. Sikap kerja yang diperlukan

4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi

4.2 Teliti dalam perolehan dan pengolahan sumber data produk kriptografi

5. Aspek kritis

5.1 Ketepatan dalam menyusun dokumentasi implementasi produk kriptografi yang sesuai dengan format dan sistematika

KODE UNIT : **J.61KRP00.011.1**

JUDUL UNIT : **Menyusun Panduan Penggunaan Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun panduan penggunaan produk kriptografi melalui identifikasi mekanisme penggunaan dan perumusan panduan penggunaan produk kriptografi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi metode penggunaan produk kriptografi	1.1 **Tahapan penggunaan produk kriptografi** diuraikan sesuai dengan dokumentasi implementasi produk kriptografi. 1.2 **Metode penggunaan produk kriptografi** dalam setiap tahapan dikompilasi sebagai panduan penerapan produk kriptografi.
2. Merumuskan panduan penggunaan produk kriptografi	2.1 **Format dan sistematika panduan** diidentifikasi sesuai dengan kebutuhan. 2.2 Panduan penggunaan produk kriptografi dibuat sesuai dengan format dan sistematika. 2.3 **Pengesahan panduan penggunaan produk kriptografi** dilakukan sesuai dengan kebutuhan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengidentifikasi mekanisme dan merumuskan panduan penggunaan produk kriptografi.
   1.2 Tahapan penggunaan produk kriptografi adalah urutan penggunaan produk kriptografi berdasarkan pemodelan, integrasi fungsi kriptografi dan pendukungnya, rancangan teknis, hasil *unit testing*, serta hasil *integration testing* pada produk kriptografi.
   1.3 Metode penggunaan produk kriptografi adalah cara atau teknik yang harus dilakukan dalam rangka penggunaan produk kriptografi.

1.4 Format dan sistematika panduan adalah susunan, urutan, klasifikasi dan pengelompokkan tertentu yang digunakan dalam penyusunan panduan penggunaan produk kriptografi.

1.5 Pengesahan panduan penggunaan produk kriptografi meliputi proses reviu kesesuaian terhadap format dan sistematika serta penandatanganan hasil penyusunan panduan penggunaan produk kriptografi oleh pembuat panduan.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 Internet

2.2 Perlengkapan

2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

(Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan

peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

1.4 Hasil unjuk kerja berupa panduan penggunaan produk kriptografi sesuai format dan secara sistematis.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Produk kriptografi

3.2 Keterampilan

3.2.1 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai prosedur penggunaan produk kriptografi

4. Sikap kerja yang diperlukan

4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi

4.2 Teliti dalam menjabarkan tahapan penggunaan produk kriptografi

5. Aspek kritis

5.1 Ketepatan dalam membuat prosedur penggunaan produk kriptografi

KODE UNIT : **J.61KRP00.012.1**

JUDUL UNIT : **Menentukan Metode Pengujian yang akan Dilakukan**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menentukan metode pengujian yang akan dilakukan melalui identifikasi informasi yang relevan dan penelaahan kesesuaian serta pemilihan metode pengujian terhadap desain produk kriptografi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi informasi yang relevan terkait dengan desain produk kriptografi yang akan diuji	1.1 Informasi terkait **desain** dan **teknik implementasi** pada produk kriptografi dikumpulkan sesuai ruang lingkup pengujian. 1.2 Informasi terkait **tren serangan** terhadap *platform* yang digunakan pada desain produk kriptografi dihimpun sesuai dengan kebutuhan pengujian. 1.3 Informasi ***best practice*** metode pengujian dihimpun sesuai dengan desain produk kriptografi.
2. Menelaah kesesuaian metode pengujian terhadap desain produk kriptografi	2.1 **Komponen penyusun produk kriptografi** yang berpotensi memiliki kelemahan diidentifikasi sesuai dengan desain produk kriptografi. 2.2 *Best practice* metode pengujian dianalisis sesuai dengan potensi kelemahan pada komponen penyusun produk kriptografi yang teridentifikasi. 2.3 **Sumber daya internal** ditentukan kesesuaiannya berdasarkan kebutuhan komputasi pengujian.
3. Memilih metode pengujian	3.1 Metode pengujian ditetapkan berdasarkan hasil telaah kesesuaian metode pengujian. 3.2 Parameter pengujian ditetapkan berdasarkan metode pengujian.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengumpulkan informasi yang relevan, mengidentifikasi kesesuaian, dan memilih metode pengujian terhadap produk kriptografi yang akan diuji.
   1.2 Desain yang dimaksud merupakan desain produk kriptografi berupa protokol kriptografi, struktur algoritma kriptografi, batasan kriptografi pada modul kriptografi.
   1.3 Teknik implementasi yang dimaksud meliputi teknik penerapan fungsi penyusun algoritma kriptografi, penerapan pada bahasa pemrograman, dan penerapan pada suatu platform.
   1.4 Tren serangan yang dimaksud merupakan serangan terhadap desain algoritma, kelemahan implementasi protokol kriptografi pada produk kriptografi, kesalahan implementasi dalam bahasa pemrograman yang digunakan, dan serangan terhadap platform yang digunakan.
   1.5 *Best practice* dalam konteks metode pengujian yang dimaksud adalah informasi terkait metode atau teknik yang dapat digunakan untuk menunjukan kelemahan atau kerentanan pada suatu produk kriptografi.
   1.6 Komponen penyusun produk kriptografi yang dimaksud meliputi algoritma kriptografi, implementasi protokol kriptografi, metode implementasi produk kriptografi, dan platform yang digunakan pada implementasi produk kriptografi.
   1.7 Sumber daya internal yang dimaksud meliputi waktu, *tools*, sumber daya manusia, dan lainnya.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

   (Tidak ada.)

4. Norma dan standar

   4.1 Norma

   (Tidak ada.)

   4.2 Standar

   4.2.1 SNI ISO/IEC 19790:2015 Teknologi informasi - Teknik keamanan – Persyaratan keamanan untuk modul kriptografi

   4.2.2 SNI 8542:2018 ISO/IEC 24759:2017 Teknologi informasi - Teknik keamanan – Persyaratan uji modul kriptografi

   4.2.3 SNI ISO/IEC 20540:2018 Teknologi informasi – Teknik keamanan – Pengujian modul kriptografi di lingkungan operasional

   4.2.4 ISO/IEC 15408-1:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

   4.2.5 ISO/IEC 15408-2:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

   4.2.6 ISO/IEC 15408-3:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

   4.2.7 ISO/IEC 15408-4:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

   4.2.8 ISO/IEC 15408-5:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

   4.2.9 ISO/IEC 18045:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.
   1.4 Hasil unjuk kerja berupa dokumen yang memuat rincian metode pengujian dan parameter pengujian pada produk kriptografi.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Persyaratan keamanan modul kriptografi
      3.1.2 Metode serangan pada modul kriptografi
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata

4. Sikap kerja yang diperlukan
   4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi
   4.2 Teliti dalam mengidentifikasi potensi kelemahan pada desain produk kriptografi

4.3 Obyektif dalam menelaah *best practice* metode pengujian

4.4 Bertanggung jawab dalam menentukan metode pengujian

5. Aspek kritis

5.1 Ketepatan dalam menentukan metode pengujian berdasarkan hasil identifikasi kesesuaian metode pengujian

KODE UNIT : **J.61KRP00.013.1**

JUDUL UNIT : **Menyusun Skenario Pengujian Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun skenario pengujian produk kriptografi melalui analisis metode pengujian dan perumusan skenario pengujian.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menganalisis metode pengujian	1.1 Metode pengujian ditelaah sesuai dengan **kebutuhan pengujian**. 1.2 Parameter pengujian ditelaah sesuai dengan metode pengujian.
2. Merumuskan skenario pengujian	2.1 **Skenario pengujian** didesain sesuai dengan hasil telaah metode pengujian. 2.2 Skenario pengujian diverifikasi sesuai dengan spesifikasi desain produk kriptografi. 2.3 ***Test case*** diidentifikasi berdasarkan skenario pengujian yang terverifikasi. 2.4 Hasil yang diharapkan/*expected value* disusun berdasarkan *test case*. 2.5 Skenario pengujian dikompilasi berdasarkan *test case* dan *expected value*.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menganalisis metode dan merumuskan skenario pengujian terhadap produk kriptografi.
   1.2 Kebutuhan pengujian yang dimaksud meliputi berbagai pertimbangan yang berkaitan dengan jenis algoritma kriptografi, desain dan teknik implementasi, tren serangan, serta informasi *best practice*.
   1.3 Skenario pengujian yang dimaksud merupakan skenario atau gambaran proses yang diperlukan untuk memastikan kesesuaian implementasi desain terhadap tujuan desain produk yang dibuat. Termasuk dalam hal ini adalah kesesuaiannya dengan aspek

keamanan yang dituju. Skenario pengujian merupakan dokumen kolektif yang memuat berbagai macam *test case*.

1.4 *Test case* adalah rancangan atau tindakan yang dilakukan oleh *user* untuk melakukan verifikasi terhadap fungsi tertentu pada produk kriptografi. *Test case* bersifat spesifik.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 Internet

2.2 Perlengkapan

2.2.3 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.3 Norma

(Tidak ada.)

4.4 Standar

4.2.1 SNI 8542:2018 ISO/IEC 24759:2017 Teknologi informasi – Teknik keamanan – Persyaratan uji modul kriptografi

4.2.2 SNI ISO/IEC 15408-1:2014 Teknologi informasi - Teknik keamanan - Kriteria evaluasi keamanan teknologi informasi - Bagian 1: Pengantar dan model umum

4.2.3 SNI ISO/IEC 18045:2015 Teknologi informasi - Teknik keamanan - Metodologi untuk evaluasi keamanan TI

4.2.4 ISO/IEC 15408-1:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

4.2.5 ISO/IEC 15408-2:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

4.2.6 ISO/IEC 15408-3:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

4.2.7 ISO/IEC 15408-4:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

4.2.8 ISO/IEC 15408-5:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

4.2.9 ISO/IEC 18045:2022 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

   1.4 Hasil unjuk kerja berupa skenario pengujian produk kriptografi.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
    3.3 Pengetahuan
        3.3.1 Metode pengujian kriptografi
        3.3.2 Metode penyusunan skenario pengujian
        3.3.3 Metode penyusunan *test case*
    3.4 Keterampilan
        3.4.1 Menyusun narasi yang empiris dan mudah dipahami pada skenario pengujian dan *test case*
4. Sikap kerja yang diperlukan
    4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi
    4.2 Teliti dalam menelaah kebutuhan pengujian
    4.3 Bertanggung jawab dalam menyusun skenario pengujian
    4.4 Obyektif dalam menyusun hasil yang diharapkan/*expected value*

5. Aspek kritis
    5.1 Ketepatan dalam memverifikasi skenario pengujian sesuai dengan spesifikasi desain produk kriptografi

KODE UNIT : **J.61KRP00.014.1**

JUDUL UNIT : **Melakukan Pengujian Terhadap Produk Kriptografi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan pengujian terhadap produk kriptografi melalui penyiapan, pelaksanaan dan perumusan hasil pengujian.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyiapkan pengujian	1.1 **Dokumen uji** dikumpulkan sesuai kebutuhan pengujian. 1.2 Perangkat pendukung pengujian diinventarisasi sesuai kebutuhan uji.
2. Menjalankan tahapan pengujian	2.1 Tahapan pengujian diidentifikasi berdasarkan *test case* pengujian. 2.2 Pengujian diterapkan berdasarkan *test case* pengujian.
3. Merumuskan hasil pengujian	3.1 Data hasil pengujian dianalisis sesuai dengan metode pengujian. 3.2 Kesimpulan ditentukan berdasarkan olah data hasil pengujian. 3.3 Laporan hasil pengujian didokumentasikan berdasarkan data pengujian.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menyiapkan kebutuhan pengujian, menjalankan tahapan dan merumuskan hasil pengujian.
   1.2 Dokumen uji yang dimaksud meliputi informasi terkait metode pengujian, skenario pengujian, dan *test case* pengujian.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Simulator produk kriptografi

2.1.3 Peralatan pendukung pengujian sesuai karakteristik produk kriptografi

2.1.4 Internet

2.2 Perlengkapan

2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

(Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi tes tertulis, demonstrasi/simulasi, metode tes lisan wawancara, observasi tempat kerja, verifikasi bukti/portofolio dan metode lain yang relevan.

1.4 Hasil unjuk kerja berupa laporan hasil pengujian.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
    3.1 Pengetahuan
        3.1.1 Metode pengujian kriptografi
    3.2 Keterampilan
        3.2.1 Menggunakan perangkat komputasi
        3.2.2 Menggunakan simulator produk kriptografi
4. Sikap kerja yang diperlukan
    4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi
    4.2 Teliti dalam mengumpulkan hasil pengujian produk kriptografi yang telah dilakukan
    4.3 Obyektif dalam melaksanakan pengujian produk kriptografi
    4.4 Bertanggung jawab dalam merumuskan hasil pengujian produk kriptografi

5. Aspek kritis
    5.1 Kecermatan dalam menganalisis data hasil pengujian sesuai dengan metode pengujian yang ditetapkan

KODE UNIT : **J.61KRP00.015.1**

JUDUL UNIT : **Menyusun Rekomendasi Berdasarkan Hasil Pengujian**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun rekomendasi berdasarkan hasil pengujian melalui identifikasi kerentanan, identifikasi kebutuhan perbaikan dan rekomendasi perbaikan terhadap produk kriptografi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi kerentanan produk kriptografi	1.1 Kerentanan pada produk kriptografi dianalisis berdasarkan hasil pengujian dan *best practice*. 1.2 Kekuatan keamanan produk kriptografi dirumuskan berdasarkan hasil analisis celah keamanan.
2. Mengidentifikasi kebutuhan perbaikan produk kriptografi	2.1 Referensi *best practice* dalam strategi perbaikan produk kriptografi diidentifikasi sesuai dengan hasil pengujian. 2.2 Hasil identifikasi kebutuhan perbaikan dianalisis berdasarkan kerentanan yang terdapat pada produk kriptografi.
3. Membuat rekomendasi perbaikan terhadap produk kriptografi	3.1 **Rekomendasi perbaikan** disusun berdasarkan kerentanan produk kriptografi. 3.2 Dokumentasi hasil rekomendasi dikomunikasikan kepada **pemangku kepentingan.**

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengidentifikasi kerentanan serta kebutuhan perbaikan dan membuat rekomendasi perbaikan terhadap produk kriptografi.
   1.2 Rekomendasi perbaikan yang dimaksud meliputi rekomendasi perbaikan aspek preventif dan aspek korektif.

1.2.1 Aspek preventif, misalnya untuk memperkuat aspek kerahasiaan dapat direkomendasikan untuk menjalankan prosedur klasifikasi informasi pada data yang dikelola melalui produk kriptografi. Atau dapat berupa rekomendasi untuk menerapkan ketentuan *back up* data secara simultan pada lokasi yang berbeda. Rekomendasi yang diberikan dapat berupa penambahan prosedur, perbaikan mekanisme dan sebagainya namun tidak diperlukan perubahan pada desain.

1.2.2 Aspek korektif, misalnya pada saat dilakukan *pentesting* ditemukan adanya celah kerawanan pada protokol yang dipilih, atau celah kerawanan pada mekanisme manajemen kuncinya. Maka, rekomendasi yang diberikan berupa penyesuaian dan perbaikan pada desain.

1.3 Pemangku kepentingan antara lain, tetapi tidak terbatas pada pimpinan organisasi, pendesain kriptografi, dan pengguna produk kriptografi.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 Internet

2.2 Perlengkapan

2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

(Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.
   1.4 Hasil unjuk kerja berupa dokumen rekomendasi perbaikan yang disusun berdasarkan kerentanan produk kriptografi.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Kekuatan keamanan produk kriptografi
      3.1.2 Strategi perbaikan produk kriptografi
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata
      3.2.2 Menyusun narasi yang empiris dan mudah dipahami kepada pemangku kepentingan

4. Sikap kerja yang diperlukan
   4.1 Berintegritas dalam menjaga keamanan informasi yang terkait dengan rencana pengembangan produk kriptografi

4.2 Teliti dalam mengidentifikasi kebutuhan perbaikan produk kriptografi

4.3 Obyektif dalam merumuskan kekuatan keamanan produk kriptografi

4.4 Tanggung jawab dalam membuat rekomendasi perbaikan produk kriptografi

5. Aspek kritis

5.1 Ketepatan dalam menyusun rekomendasi perbaikan berdasarkan kerentanan produk kriptografi

BAB III
PENUTUP

Dengan ditetapkannya Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Telekomunikasi Bidang Kriptografi, maka SKKNI ini menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH