III. CONTOH SURAT PERNYATAAN ANGGOTA DIREKSI DAN KOMISARIS

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama :

NIK :

Tempat/tanggal lahir :

Alamat :

dalam hal ini bertindak dalam jabatan saya selaku [anggota Direksi atau Komisaris] [Nama Lembaga Selain Bank] dengan ini menyatakan bahwa sebelum dan/atau pada saat mengajukan permohonan ini:

1. Saya tidak pernah dinyatakan pailit atau menjadi anggota Direksi atau Komisaris yang dinyatakan bersalah menyebabkan suatu badan usaha dinyatakan pailit dalam waktu 5 (lima) tahun sebelum tanggal Surat Pernyataan ini saya buat;
2. Saya tidak pernah dihukum atas tindak pidana di bidang perbankan, keuangan, dan/atau pencucian uang berdasarkan putusan pengadilan yang telah memiliki kekuatan hukum yang tetap;
3. Saya tidak tercantum dalam daftar kredit macet; dan
4. Saya tidak pernah masuk dalam daftar hitam nasional penarik cek/bilyet giro kosong yang ditatausahakan Bank Indonesia.

Demikian Surat Pernyataan ini saya buat dengan sesungguhnya dan saya bersedia serta mematuhi segala tindakan dan/atau keputusan yang diambil oleh Bank Indonesia, termasuk namun tidak terbatas pada permintaan pengunduran diri saya apabila dikemudian hari terbukti pernyataan saya dalam Surat Pernyataan ini tidak benar.

[Kota], [Tanggal Bulan Tahun]

Yang membuat pernyataan,

MATERAI

Rp6000,00

[Nama Lengkap]

IV. PEDOMAN PENYELENGGARAAN UANG ELEKTRONIK DENGAN MENGGUNAKAN MEDIA *CHIP*

A. Pendahuluan

1. Latar Belakang

Aktivitas penggunaan Uang Elektronik dengan menggunakan teknologi *Chip* oleh masyarakat meningkat pesat sejak diterbitkan pertama kali pada tahun 2007. Perkembangan ini menunjukkan potensi Uang Elektronik sebagai instrumen pembayaran di masa datang cukup baik. Penerimaan Uang Elektronik sebagai instrumen pembayaran saat ini tidak lagi terbatas hanya pada sektor ritel namun juga pada sektor publik, seperti transportasi dan pembayaran tagihan (*billing*). Mempertimbangkan potensi Uang Elektronik tersebut, Bank Indonesia terus berupaya untuk meningkatkan keamanan dan kelancaran penyelenggaraan Uang Elektronik. Kedua hal ini dibutuhkan untuk meningkatkan kepercayaan masyarakat dalam bertransaksi non tunai menggunakan Uang Elektronik, terutama dari aspek pengamanan instrumen dan kepastian penyelesaian transaksi Uang Elektronik.

Di sisi lain, Bank Indonesia menginginkan industri Uang Elektronik yang lebih efisien dan luas jangkauan layanannya, dengan melakukan interkoneksi penyelenggaraan Uang Elektronik dan membuka peluang bisnis secara non eksklusif, terutama pada berbagai sektor bisnis yang strategis. Untuk itu Bank Indonesia menyamakan arah pengembangan Uang Elektronik dengan penggunaan standar teknis dan mekanisme yang mendukung interkoneksi.

Meninjau latar belakang dan inisiatif Bank Indonesia untuk meningkatkan keamanan dan efisiensi, kelancaran penyelenggaraan, serta memperluas jangkauan layanan, Bank Indonesia menerbitkan Pedoman Penyelenggaraan Uang Elektronik Dengan Menggunakan *Chip* yang selanjutnya disebut sebagai “Pedoman Uang Elektronik Menggunakan *Chip*”.

Pedoman ini berisikan materi teknis penyelenggaraan Uang Elektronik yang menggunakan *Chip*.

2. Prinsip Implementasi

a. Cakupan Teknis

Pedoman Uang Elektronik menggunakan *Chip* diimplementasikan pada Uang Elektronik yang penyimpanan nilai uangnya menggunakan media *Chip*.

b. Definisi Umum

1) *Card reader* : Perangkat pembaca data dari *Chip card*.

2) *Chip card* : Dikenal juga sebagai IC (*Integrated Circuit*) *card*, adalah kartu yang mengandung 1 (satu) atau lebih *computer Chip* atau IC untuk identifikasi, penyimpanan data atau proses tertentu untuk kepentingan validasi PIN, otorisasi transaksi pembayaran verifikasi saldo dan menyimpan data-data personal.

3) *Contact card* : Kartu sistem dengan *Chip* dimana penampang *Chip* terlihat pada permukaan kartu, memiliki sistem operasi, dan aplikasi sehingga penggunaannya (pembacaan aplikasi dan data) hanya dapat dilakukan dengan memasukkan (insersi) kartu sistem tersebut kepada terminal atau alat pembacanya.

4) *Contactless card* : Kartu sistem dengan *Chip* di dalamnya, memiliki sistem operasi, aplikasi, dan rangkaian

			catudaya pemancar gelombang radio (RFID) untuk saling bertukar informasi sehingga dalam penggunaannya tidak perlu melalui kontak fisik dengan terminal atau alat pembacanya (*card reader*).
5)	*Fraud*	:	Kecurangan atau tindak pidana melanggar hukum yang dilakukan untuk mendapatkan keuntungan.
6)	*Interface*	:	Batas antara dua sistem independen (dalam hal ini, antara *smart card* dan *card reader*) untuk bertemu dan berkomunikasi satu sama lain.
7)	*Offline*	:	Interaksi penuh yang terjadi antara aplikasi dalam *smart card* dan *security access module* tanpa melibatkan konfirmasi interaksi dengan *host* Penerbit.
8)	*Online*	:	Interaksi antara aplikasi dalam *Chip smart card* dan *host* Penerbit.
9)	*Magnetic stripe*	:	Pita magnetik yang memiliki kemampuan untuk menyimpan data dengan menggunakan prinsip *electromagnetic*.
10)	*Top up*	:	Penambahan nilai uang elektronik pada uang elektronik.
11)	Lembaga Penyelenggara Interoperabilitas (*Trusted Service Manager-TSM*)	:	Lembaga yang dipercaya oleh seluruh peserta/anggota suatu sistem yang berfungsi sebagai melakukan menjaga kemanan dan pengelolaan.
12)	Uang Elektronik	:	Uang Elektronik yang

dengan Menggunakan Media *Chip*	menggunakan media *Chip* sebagai penyimpan nilai uang.

B. Persyaratan Teknis

1. Standar Fisik (*Physical Characteristics*)

a. Uang Elektronik menggunakan *Chip* yang menggunakan antarmuka kontak harus sesuai dengan standar ISO/IEC 7816.

b. Uang Elektronik menggunakan *Chip* yang menggunakan antarmuka nir-kontak harus sesuai dengan standar ISO/IEC 14443.

2. Minimum Waktu Proses Baca Data dan Informasi (*Transaction Performance*)

a. Metode *Contact*

Proses baca dan tulis data transaksi Uang Elektronik dengan metode *contact* harus dapat diselesaikan dalam waktu kurang dari 2 detik atau 2000 milidetik.

b. Metode *Contactless*

Proses baca dan tulis data transaksi Uang Elektronik dengan metode *contactless* harus dapat diselesaikan dalam waktu kurang dari 1 detik atau 1000 milidetik.

3. Pengamanan Data dan Informasi (*Data and Information Security*)

a. Integritas Data (*Integrity*)

1) Integritas data harus dapat dipastikan untuk data transaksi dan Nilai Uang Elektronik.
2) Nilai Uang Elektronik menggunakan *Chip* yang disimpan harus dapat dibuktikan kebenarannya.
3) Nilai Uang Elektronik menggunakan *Chip* berubah sesuai transaksi yang dilakukan oleh pemegang dalam hal ini

berasal dari Pengisian Ulang (*top up*), pembayaran, dan transfer dana.

4) Data transaksi Uang Elektronik menggunakan *Chip* yang diproses memiliki kode unik yang dapat dikenali atau diidentifikasikan sebagai data asli yang berasal dari Penerbit.
5) Kode unik digunakan secara konsisten pada setiap transaksi.

b. Kerahasiaan Data (*Confidentiality*)

1) Data transaksi Uang Elektronik menggunakan *Chip* diperlakukan sebagai data yang sangat rahasia.
2) Pengelolaan data transaksi Uang Elektronik menggunakan *Chip* dilakukan sesuai dengan prosedur standar kerahasiaan yang dipatuhi oleh seluruh Penyelenggara Uang Elektronik menggunakan *Chip* dan pihak yang dinyatakan berkepentingan dalam Penyelenggara Uang Elektronik menggunakan *Chip*.

c. Identifikasi Peran dan Pemantauan (*Role Identification and Monitoring*)

Setiap Penyelenggara Uang Elektronik menggunakan *Chip* melakukan identifikasi peran dan pemantauan terhadap aktivitas seluruh pihak yang bekerjasama dalam penyelenggaraan Uang Elektronik menggunakan *Chip*, dengan cara:

1) meminta laporan berkala dari pihak yang bekerjasama dengan Penyelenggara mengenai aktivitas penyelenggaraan Uang Elektronik menggunakan *Chip*, yang meliputi kinerja, keamanan, serta penyelesaian permasalahan dan gangguan dalam penyelenggaraan Uang Elektronik menggunakan *Chip*;
2) menuangkan dalam SOP pihak yang bekerjasama mengenai kewajiban pemantauan penyelenggaraan Uang Elektronik menggunakan *Chip*;

3) menuangkan hak dan kewajiban Penyelenggara dan pihak yang bekerjasama dalam perjanjian tertulis;
4) meminta pihak yang bekerjasama melakukan audit keamanan secara berkala.

d. Otentikasi (*Authentication*)

1) Setiap transaksi Uang Elektronik menggunakan *Chip* dan kegiatan pertukaran data penyelenggaraan Uang Elektronik menggunakan *Chip* dilakukan autentikasi.
2) Autentikasi transaksi Uang Elektronik menggunakan *Chip* dilakukan dengan fitur autentikasi pada *Chip* untuk memastikan keaslian data dan informasi transaksi Uang Elektronik menggunakan *Chip*.
3) Masing-masing proses transaksi Uang Elektronik menggunakan *Chip,* yang berupa aktivitas debet dan kredit nilai uang elektronik dilakukan autentikasi.
4) Kegiatan pengiriman laporan data transaksi dari sistem Uang Elektronik menggunakan *Chip* kepada pihak-pihak yang berwenang dalam penyelenggaraan Uang Elektronik menggunakan *Chip* dilakukan autentikasi, dan begitu pula sebaliknya.

e. Pengelolaan Akses (*Access Control*)

1) Seluruh akses penyelenggaraan Uang Elektronik menggunakan *Chip* ditetapkan kewenangan secara berjenjang.
2) Seluruh akses terhadap data dan informasi penyelenggaraan Uang Elektronik menggunakan *Chip* hanya diberikan kepada pihak yang berkepentingan.

f. Keberlangsungan Proses Transaksi (*Atomicity*)

1) Penerbit harus menyelesaikan proses transaksi Uang Elektronik menggunakan *Chip* secara lengkap.

2) Dalam hal proses tersebut mengalami gangguan atau kegagalan, transaksi Uang Elektronik menggunakan *Chip* harus dibatalkan.

g. Batasan Nilai Transaksi (*Value Limitations*)

1) Eksekusi transaksi dalam sistem Uang Elektronik menggunakan *Chip* dibatasi nilainya sesuai ketentuan yang berlaku.
2) Limitasi berupa maksimum transaksi dan maksimum Nilai Uang Elektronik dalam Uang Elektronik menggunakan *Chip*.

h. Penyimpanan dan Penelusuran Data dan Informasi (*Traceability*)

1) Jangka waktu penyimpanan data dan informasi transaksi Uang Elektronik menggunakan *Chip* dalam *database* utama (*main database*) paling kurang 12 (dua belas) bulan.
2) Jangka waktu penyimpanan data dan informasi transaksi Uang Elektronik menggunakan *Chip* dalam *Chip* yang diproses secara *offline* paling kurang 10 (sepuluh) transaksi terakhir.
3) Seluruh data strategis dalam penyelenggaraan Uang Elektronik menggunakan *Chip* yang meliputi penggantian, peningkatan kualitas dan kapasitas, modifikasi, penambahan, dan pengurangan sistem penyelenggaraan Uang Elektronik menggunakan *Chip* disimpan untuk kepentingan audit keamanan.

i. Deteksi terhadap *Fraud* (*Fraud Detection*)

Sistem penyelenggaraan Uang Elektronik menggunakan *Chip* memiliki kemampuan untuk:

1) melakukan deteksi terhadap kejadian abnormal termasuk *fraud* dan termasuk kejadian *fraud* yang berasal dari

data breach/percobaan pengaksesan data dan informasi rahasia oleh pihak-pihak yang tidak berkepentingan;

2) menyampaikan informasi kepada pihak yang berkepentingan mengenai kejadian abnormal dalam bentuk *dashboard indicator*.

j. Reaksi terhadap *Fraud* (*Fraud Reaction*)

Dalam hal terjadi *fraud*:

1) Sistem Uang Elektronik menggunakan *Chip* mampu membatasi kejadian *fraud* atau tidak melanjutkan proses transaksi Uang Elektronik menggunakan *Chip*; dan
2) Sistem Uang Elektronik menggunakan *Chip* mampu mengisolir dampak *fraud* secara luas.

k. Kriptografi dan Protokol (*Cryptography* dan *Protocols*)

1) Proses transaksi Uang Elektronik menggunakan *Chip* dilakukan dengan:
   a) menggunakan algoritma kriptografi terkini yang telah terstandardisasi secara internasional, diketahui dan teruji secara luas oleh publik; dan
   b) menggunakan jaringan komunikasi yang dilengkapi dengan protokol dan prosedur keamanan terkini yang telah terstandardisasi secara internasional.
2) Proses transaksi Uang Elektronik menggunakan *Chip* dilarang menggunakan algoritma kriptografi yang bersifat *private*.

l. Pengelolaan *Key*

Pengelolaan kerahasiaan dan integritas *key* dilakukan melalui pembentukan, distribusi, proteksi, penetapan *life cycle,* dan pengkinian secara berkala. Prosedur pengelolaan key dilakukan sebagai berikut:

1) Terdapat standarisasi dalam proses pembentukan dan distribusi *key*.

2) *Key* dibentuk melalui suatu proses yang sedemikian dijaga kerahasiaannya.
3) Tiap-tiap *key* ditentukan *life cycle*-nya sesuai kebutuhan penyelenggaraan.
4) Terdapat mekanisme penggantian *key* apabila diperlukan.
5) Tiap *key* yang didedikasikan untuk satu fungsi keamanan hanya digunakan untuk fungsi tersebut.
6) *Key* ditransportasikan dan disimpan dalam perangkat yang tahan terhadap upaya-upaya perusakan dan peretasan.

m. *Trusted Path*

1) Jalur komunikasi yang digunakan dalam penyelenggaraan Uang Elektronik harus dilindungi dengan perangkat pengamanan.
2) Semua jalur yang digunakan untuk melakukan pertukaran transaksi, akses data harus dipastikan tidak dapat diakses oleh pihak-pihak dan/atau aplikasi yang tidak berkepentingan.

n. *Trusted Location*

1) Media penyimpanan data dan informasi transaksi Uang Elektronik dalam media penyimpanan data yang ditempatkan pada lokasi yang terjaga keamannya.
2) Akses ke lokasi tersebut hanya diberikan kepada pihak-pihak yang berkepentingan.
3) Pengamanan lokasi dilakukan dengan pengamanan fisik dan akses.

o. Kompetensi dan Tanggung Jawab (*Competence and Responsibility*)

1) Penyelenggaraan Uang Elektronik didukung oleh sumber daya manusia yang:

a) memiliki pengetahuan dan kompetensi teknis mengenai penyelenggaraan Uang Elektronik secara lengkap;
b) mengetahui informasi secara lengkap untuk menjalankan perannya dalam penyelenggaraan Uang Elektronik; dan
c) mematuhi kewajibannya dalam menjalankan operasional penyelenggaraan Uang Elektronik.

2) Penyelenggara menyediakan pelatihan yang memadai kepada seluruh personil yang menangani sistem penyelenggaraan Uang Elektronik, yang bertujuan untuk memitigasi gangguan atau kegagalan sistem karena *human error.*

p. Pengujian Sistem (*Qualification and Tests*)

1) Pengujian sistem penyelenggaraan harus dilakukan secara lengkap terhadap komponen sistem, sejak, sebelum, dan/atau selama pengoperasian sistem untuk menjamin keandalan sistem.
2) Setiap pengujian sistem penyelenggaraan Uang Elektronik harus dinyatakan layak yang dibuktikan dengan hasil audit keamanan.
3) Penyelenggara harus melakukan audit keamanan terhadap sistem penyelenggaraan Uang Elektronik secara berkala dan kontinu.

q. Asesmen Terhadap Perangkat Pengamanan (*Security Assessment*)

Penyelenggara senantiasa memastikan pihak-pihak yang memiliki kepentingan terhadap sistem Uang Elektronik menggunakan *Chip* melakukan tindakan terkait penyelenggaraan Uang Elektronik menggunakan *Chip* sesuai dengan prosedur pengamanan yang berlaku.

r. Pengkinian Perangkat Pengamanan (*Security Update*)

Penyelenggara melakukan pengkinian terhadap seluruh komponen pengamanan sistem Uang Elektronik yang dinilai sensitif secara berkala dan kontinu.

s. *Availability*

Penyelenggara menjamin ketersediaan penyelenggaraan Uang Elektronik menggunakan *Chip* pada tingkat paling rendah 99%.

t. Siklus Hidup (*Life Cycle*)

Penyelenggara memiliki prosedur pengamanan yang memadai sepanjang Uang Elektronik dinyatakan tersebut masih dapat digunakan oleh pemegang.

u. Partisi (*Partion*)

Penyelenggara menyediakan partisi yang jelas untuk memisahkan aplikasi pendukung dari aplikasi utama sistem Uang Elektronik.

4. Interoperabilitas

Interoperabilitas antara Penyelenggara dilakukan melalui lembaga penyelenggara interoperabilitas/*Trusted Service Management* (TSM).