LAMPIRAN
SURAT EDARAN DIREKTUR JENDERAL PAJAK
NOMOR : SE-56/PJ/2011
TENTANG : PEDOMAN ENKRIPSI DAN *KEY MANAGEMENT*

Pedoman Enkripsi dan *Key Management*

Direktorat Jenderal Pajak
Kementerian Keuangan Republik Indonesia

Versi 1.0

Klasifikasi : TERBATAS

Tanggal : 9 Agustus 2011

Diterbitkan oleh :
Direktorat Jenderal Pajak

LEMBAR PENGENDALIAN

NO	Penerima Dokumen	Format Dokumen
1	Direktorat TTKI	Cetakan
2	Direktorat TIP	Cetakan
3	Direktorat KITSDA	Cetakan
4	Direktorat TPB	Cetakan
5	PPDDP	Cetakan
6	Pegawai DJP	Elektronik

HALAMAN REVISI

Bab/Sub-Bab	Halaman	Revisi	Tanggal	Uraian Revisi
		V.1.0	09/08/2011	

DAFTAR ISI

A. Deskripsi :

Pedoman Enkripsi dan *Key Management* disusun dengan tujuan untuk memberi panduan serta aturan dalam pemanfaatan enkripsi dan metode kriptografi lainnya yang diperlukan untuk menjaga data/informasi elektronik yang diklasifikasikan rahasia atau sangat rahasia berdasarkan Kebijakan Pengelolaan Keamanan Informasi DJP (selanjutnya disebut dengan data atau informasi sensitif) khususnya pada aspek kerahasiaan, keutuhan, otentikasi, dan jaminan pengakuan oleh pemilik informasi (*non-repudiation*).

Penerapan enkripsi dalam rangka menjamin keamanan transaksi data atau informasi sensitif melibatkan penggunaan kunci kriptografi, untuk menjamin keandalan dari kunci kriptografi tersebut diperlukan penerapan *key management* yang mengatur mulai dari penerbitan pasangan kunci (publik-pribadi), pendistribusian, sampai dengan penghapusannya.

Berdasarkan hal tersebut di atas maka Pedoman Enkripsi dan *Key Management* mengatur hal-hal sebagai berikut :

1. Ketentuan mengenai penerapan enkripsi dalam aktivitas berikut ini:
   a. Pengiriman data/informasi sensitif;
   b. Penyimpanan data/informasi sensitif;
   c. Pemanfaatan *Secure Socket Layer (SSL)* untuk mengamankan akses terhadap data/informasi sensitif.

2. Ketentuan mengenai *key management* yang meliputi proses berikut ini:
   a. Penerbitan serta penyimpanan pasangan kunci dan sertifikat elektronik;
   b. Penyebaran kunci publik dan sertifikat elektronik;
   c. Penggunaan pasangan kunci dan sertifikat elektronik;
   d. Pembatalan keabsahan serta penghapusan kunci publik dan sertifikat elektronik;
   e. Penerbitan kembali pasangan kunci dan sertifikat elektronik;
   f. *Backup* dan *restore* sistem pengelolaan kunci kriptografi;
   g. *Cross certification*.

B. Dasar Hukum dan Acuan :

1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
2. Peraturan Direktur Jenderal Pajak Nomor PER-41/PJ/2010 tentang Kebijakan Pengelolaan Keamanan Informasi Direktorat Jendral Pajak;
3. ISO/IEC 27001:2005 Klausul 12.3 tentang Pengendalian Kriptografi;
4. RFC 3467 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*.

C. Dokumen Terkait :

1. Pedoman Penggunaan *User Account*/*Password*, Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, Serta Penggunaan Akses Internet dan Intranet;
2. Pedoman *Backup* dan *Restore* Data/Sistem/Informasi;
3. Pedoman Pengelolaan Keamanan Perangkat dan Fasilitas Pengolah Informasi;
4. Pedoman Pengendalian Dokumen dan Catatan Penerapan Tata Kelola TIK DJP;
5. Pedoman Tindakan Perbaikan dan Pencegahan serta Pengelolaan Gangguan Keamanan Informasi.

D. Pedoman Enkripsi:

1. Ketentuan Umum Enkripsi

1.1. Pengguna Aset Informasi harus menerapkan mekanisme enkripsi dengan menggunakan perangkat lunak kriptografi yang ditetapkan penggunaannya di DJP untuk melindungi data/informasi sensitif yang digunakan dalam aktivitas berikut:
   1.1.1. Pengiriman data/informasi;
   1.1.2. Penyimpanan data/informasi;
   1.1.3. Akses data/informasi dalam aplikasi yang menggunakan jaringan publik (internet).

1.2. Jenis enkripsi yang digunakan adalah:
   1.2.1. Enkripsi asimetris;
   1.2.2. Enkripsi simetris.

1.3. Penentuan jenis enkripsi yang digunakan untuk setiap aktivitas pemanfaatan data atau informasi dilakukan dengan mempertimbangkan bentuk aktivitas pemanfaatan data tersebut dan ukuran data atau informasi yang akan dienkripsi tersebut. Ketentuan mengenai penggunaan jenis enkripsi asimetris dan simetris adalah sebagai berikut:
   1.3.1. Enkripsi asimetris digunakan untuk melindungi data atau informasi yang diakses atau dikirim melalui jaringan komunikasi, yang mana ukuran data atau informasi tersebut relatif kecil, misalnya dalam penggunaan e-mail, pengiriman kunci simetris melalui jaringan komunikasi data, serta akses terhadap data/informasi dalam aplikasi yang menggunakan saluran publik (internet);
   1.3.2. Enkripsi simetris digunakan untuk melindungi data atau informasi yang disimpan dalam suatu media, yang mana ukuran data atau informasi tersebut besar, misalnya dalam *back-up* data atau informasi dan penggunaan *removable media* untuk menyimpan atau mengirim data atau informasi.

1.4. Kepala Seksi Bimbingan Sistem, Direktorat Teknologi Informasi Perpajakan (TIP) bertanggung jawab untuk memberikan pelatihan kepada Pengguna Aset Informasi terkait penerapan

enkripsi dan *key management* di Direktorat Jenderal Pajak;

1.5. Kepala Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data, Direktorat TIP bertanggung jawab untuk memastikan bahwa setiap fasilitas pengolah data atau informasi sensitif yang diakses melalui jaringan komunikasi data DJP telah menggunakan lapisan protokol yang dilengkapi dengan mekanisme enkripsi dan dekripsi, misalnya: *secure socket layer* (*ssl*) dan *secure shell* (*ssh*);

1.6. Direktur Transformasi Teknologi Komunikasi dan Informasi bertanggung jawab untuk menetapkan perangkat lunak kriptografi yang digunakan untuk aktivitas sebagaimana disebutkan pada angka 1.1;

1.7. Direktur Transformasi Teknologi Komunikasi dan Informasi bertanggung jawab untuk menetapkan standar mengenai hal-hal berikut:

1.5.1. Metode kriptografi yang sesuai dengan tujuan keamanan dari setiap aktivitas penggunaan data/informasi sensitif;

1.5.2. Algoritma yang tidak boleh digunakan dalam perlindungan keamanan dengan kriptografi;

1.8. Pengelolaan pasangan kunci yang digunakan dalam enkripsi asimetris dilakukan dengan memanfaatkan teknologi *Public Key Infrastructure*.

2. Ketentuan Enkripsi Asimetris dalam Pengiriman Data/Informasi Sensitif

2.1. Pengirim menyiapkan data/informasi sensitif yang akan dienkripsi;

2.2. Pengirim mencari sertifikat elektronik milik Penerima data/informasi melalui aplikasi pengelolaan kunci yang digunakan di DJP;

2.3. Pengirim bertanggung jawab memeriksa status sertifikat elektronik milik Penerima dalam *Certificate Revocation List (CRL)*, untuk memastikan bahwa sertifikat elektronik tersebut tidak dicabut/dibatalkan keabsahannya;

2.4. Setelah meyakini bahwa sertifikat elektronik tersebut masih berlaku dan valid, Pengirim mengunduh sertifikat elektronik tersebut dari *key server* ke dalam tempat penyimpanan sertifikat elektronik miliknya;

2.5. Pengirim mengenkripsi data/informasi yang akan dikrimnya dengan menggunakan kunci publik dalam sertifikat elektronik milik Penerima;

2.6. Pengirim menandatangani secara elektronik file data/informasi yang akan dikirim dengan kunci pribadi miliknya;

2.7. Atasan langsung Pengirim mengawasi enkripsi data/informasi sensitif yang akan dikirim dengan menggunakan fungsi yang tersedia dalam aplikasi kriptografi yang digunakan di DJP, untuk kemudian memberikan persetujuan pengiriman apabila data/informasi sensitif telah terenkripsi dengan kunci kriptografi yang tepat;

2.8. Setelah mendapatkan kiriman file data/informasi yang terenkripsi, Penerima harus memeriksa validitas tanda tangan elektronik Pengirim dengan menggunakan Sertifikat Elektronik milik Pengirim yang diunduh dari *key server*;

2.9. Setelah meyakini validitas tanda tangan elektronik Pengirim, Penerima mendekripsi file data/informasi tersebut dengan menggunakan kunci pribadi yang hanya diketahui olehnya.

3. Ketentuan Enkripsi Simetris dalam Pengiriman Data atau Informasi Sensitif

3.1. Pengirim menyiapkan data/informasi sensitif yang akan dienkripsi;

3.2. Pengirim membuat *password* yang akan digunakan sebagai kunci kriptografi dalam proses enkripsi, pembuatan *password* ini harus mematuhi ketentuan dalam Pedoman Pedoman Penggunaan *User Account/Password*, Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, serta Penggunaan Akses Internet dan Intranet;

3.3. Pengirim mengenkripsi file data/informasi sensitif yang akan dikirim dengan menggunakan kunci kriptografi yang telah dibuat sebelumnya;

3.4. Pengirim mengenkripsi *password* dari file data/informasi sensitif yang akan dikirimkan kepada Penerima dengan enkripsi asimetris, yang mana pelaksanaannya telah dijelaskan pada Ketentuan Enkripsi Asimetris dalam Pengiriman Data/Informasi Sensitif dalam Pedoman ini;

3.5. Atasan langsung Pengirim mengawasi enkripsi data/informasi sensitif yang akan dikirim dengan menggunakan fungsi yang tersedia dalam aplikasi kriptografi yang digunakan di DJP, untuk kemudian memberikan persetujuan pengiriman apabila data/informasi sensitif telah terenkripsi dengan kunci kriptografi yang tepat;

3.6. Setelah menerima data/informasi serta *password* yang terenkripsi dari Pengirim, Penerima harus memeriksa validitas tanda tangan elektronik Pengirim dan mendekripsi file *password* yang diterimanya dengan menggunakan kunci pribadi yang hanya diketahui olehnya;

3.7. Setelah *password* berhasil didekripsi, Penerima menggunakan password tersebut untuk mendekripsi data/informasi yang diterimanya.

4. Ketentuan Enkripsi Simetris dalam Penyimpanan Data atau Informasi Sensitif

4.1. Penyimpan menyiapkan data/informasi sensitif yang akan dienkripsi;

4.2. Penyimpan bertanggung jawab menghitung nilai *hash* dari data/informasi yang akan disimpan, nilai *hash* ini dapat digunakan untuk menguji integritas data/informasi yang disimpan pada saat akan digunakan kembali;

4.3. Penyimpan membuat password yang akan digunakan sebagai kunci kriptografi dalam proses enkripsi, pembuatan password ini harus mematuhi ketentuan dalam Pedoman Pedoman Penggunaan *User Account/Password*, Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, serta Penggunaan Akses Internet dan Intranet;

4.4. Penyimpan mengenkripsi file data/informasi yang akan disimpan dengan menggunakan kunci kriptografi yang telah dibuat sebelumnya;

4.5. Penyimpan mengenkripsi password dan nilai hash dari data/aplikasi yang akan disimpan dengan menggunakan kunci publik milik Atasan Langsungnya;

4.6. Penyimpan menyerahkan password dan nilai *hash* yang telah dienkripsi kepada Atasan langsungnya;

4.7. Atasan langsung Pengirim mengawasi enkripsi data/informasi sensitif yang akan disimpan dengan menggunakan fungsi yang tersedia dalam aplikasi kriptografi yang digunakan di DJP,

untuk kemudian memberikan persetujuan penyimpanan apabila data/informasi sensitif telah terenkripsi dengan benar.

5. Ketentuan Enkripsi pada Akses Data/Informasi Sensitif di Dalam Aplikasi

5.1. Akses data/informasi sensitif dalam aplikasi yang menggunakan jaringan publik (internet) dilakukan dengan memanfaatkan metode koneksi yang dilengkapi dengan *secure socket layer*, Pengguna aplikasi mengakses aplikasi tersebut menggunakan protokol yang aman;

5.2. *Certificate Authority* (CA) membuat pasangan kunci dan menerbitkan sertifikat elektronik untuk aplikasi tersebut, setelah mendapatkan pemberitahuan tentang pengoperasian aplikasi yang memuat data/informasi sensitif yang aksesnya dapat dilakukan melalui jaringan publik (internet);

5.3. CA menyerahkan pasangan kunci dan sertifikat elektronik aplikasi tersebut kepada Administrator Sistem;

5.4. Administrator sistem melakukan pengaturan konfigurasi protokol, untuk menetapkan kunci publik dan kunci pribadi yang telah diterbitkan oleh CA untuk aplikasi tersebut, sebagai pasangan kunci dalam *secure socket layer;*

5.5. Administrator sistem bertanggung jawab untuk melakukan pengaturan konfigurasi aplikasi untuk hanya menerima koneksi melalui protokol yang menggunakan SSL;

5.6. CA mendistribusikan sertifikat elektronik aplikasi tersebut kepada pengguna aplikasi melalui *key server*;

5.7. Pengguna aplikasi mencari sertifikat elektronik aplikasi dan memeriksa statusnya pada CRL;

5.8. Pengguna aplikasi mengunduh sertifikat elektronik aplikasi dari *key server*;

5.9. Pengguna aplikasi meng*install* sertifikat elektronik tersebut ke dalam *browser* dan menempatkannya pada kategori sertifikat elektronik yang berasal dari penerbit yang dapat dipercaya;

5.10. Pada saat mengakses aplikasi, pengguna dapat melihat bahwa aplikasi tersebut telah diotentikasi dan koneksi ke aplikasi tersebut terenkripsi;

5.11. Apabila terdapat pesan *certificate error*, pengguna aplikasi harus memeriksa penyebab *error* tersebut dan memastikan bahwa alamat *website* aplikasi yang akan diakses adalah benar alamat yang seharusnya;

5.12. Pemantau keamanan jaringan melakukan pemantauan dan analisis terhadap paket-paket data yang ditransmisikan oleh aplikasi yang diakses melalui jaringan publik (internet) untuk memastikan bahwa tidak ada celah keamanan yang berpotensi menimbulkan gangguan keamanan dan kerugian bagi DJP.

E. Pedoman *Key Management*

1. Ketentuan Umum *Key Management*

1.1. Pedoman *Key Management* ini mengatur pengelolaan pasangan kunci dalam kriptografi asimetris;

1.2. Kunci yang digunakan dalam kriptografi simetris diperlakukan sebagai password sehingga pengelolaannya mengacu pada Pedoman Penggunaan *User Account/Password*, Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, serta Penggunaan Akses Internet dan Intranet;

1.3. Kepala Seksi Pengelolaan Intranet dan Internet, Direktorat Teknologi Informasi Perpajakan menjalankan fungsi *Certification Authority* DJP, untuk selanjutnya disebut *Certification Authority*;

1.4. Direktur Teknologi Informasi Perpajakan menunjuk Pelaksana pada Seksi Pengelolaan Intranet dan Internet untuk menjalankan fungsi *Registration Authority* DJP, untuk selanjutnya disebut *Registration Authority*;

1.5. *Certification Authority* dapat mendelegasikan sebagian wewenangnya kepada *Registration Authority*, kecuali wewenang menandatangani sertifikat elektronik;

1.6. *Certification Authority* harus memastikan bahwa:

1.6.1. Seluruh kunci kriptografi terlindungi dari perubahan yang tidak terotorisasi, kehilangan, atau kerusakan;

1.6.2. Seluruh peralatan yang digunakan dalam penerbitan, penyimpanan, dan *backup* kunci kriptografi harus terlindungi secara fisik dengan mengacu kepada Pedoman Pengamanan Perangkat dan Fasilitas Pengolah Informasi.

1.7. Pegawai, Wajib Pajak, dan pihak ketiga yang menggunakan kriptografi harus memastikan bahwa semua *password* dan kunci pribadi tidak diketahui oleh pihak yang tidak berhak;

1.8. Tata cara pembuatan dan penggunaan *password*/kunci pribadi mengacu kepada Pedoman Penggunaan *User Account*/*Password*, Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, serta Penggunaan Akses Internet dan Intranet.

2. Ketentuan Penerbitan serta Penyimpanan Pasangan Kunci dan Sertifikat Elektronik

2.1. Pegawai DJP, Wajib Pajak, dan pihak ketiga yang akan memanfaatkan kriptografi dapat diberikan pasangan kunci dan sertifikat elektronik setelah melakukan pendaftaran dan menyetujui kesepakatan tentang hak dan tanggung jawab yang dituangkan dalam *Subscriber Agreement*;

2.2. Format tampilan *Subscriber Agreement* diatur dalam Lampiran IV pada Pedoman ini;

2.3. Aplikasi yang menerapkan kriptografi untuk pemenuhan tujuan keamanan diberikan pasangan kunci dan sertifikat elektronik secara langsung oleh *Certification Authority* pada saat pengembangan aplikasi tersebut;

2.4. Pendaftaran untuk mendapatkan pasangan kunci dan sertifikat elektronik dapat diajukan melalui *Service Desk TIK*;

2.5. *Certification Authority* DJP menandatangani sertifikat elektronik dari *subscriber* yang telah mendaftar dan diverifikasi kebenaran data identitas yang disampaikannya, kemudian mempublikasikannya melalui *server* penyebaran sertifikat elektronik (*repository*) yang dapat

diakses oleh setiap pegawai di lingkungan DJP atau pihak luar yang telah diotorisasi melalui jaringan komunikasi data DJP;

2.6. Dalam rangka mencegah kerugian yang dapat ditimbulkan oleh kebocoran kunci pribadi yang dimiliki setiap *subscriber*, maka diberlakukan pembatasan masa berlaku dari setiap sertifikat elektronik dengan ketentuan sebagai berikut:

2.6.1. Sertifikat elektronik yang diterbitkan untuk pegawai DJP masa berlakunya tidak boleh melampaui 2 tahun;
2.6.2. Sertifikat elektronik yang diterbitkan untuk Wajib Pajak tidak boleh melampaui 2 tahun;
2.6.3. Sertifikat elektronik yang diterbitkan untuk pihak ketiga yang memiliki kerja sama dengan DJP tidak boleh melampaui 1 tahun;
2.6.4. Sertifikat elektronik yang diterbitkan untuk aplikasi tidak boleh melampaui 5 tahun;
2.6.5. Apabila masa berlaku sertifikat elektronik telah habis maka Pegawai, Wajib Pajak, dan pihak ketiga harus mengajukan penerbitan kembali sertifikat elektronik.

2.7. Hak dan kewajiban *subscriber* dalam penggunaan kunci pribadi dan sertifikat elektronik diatur lebih lanjut dalam *Subscriber Agreement* yang dibuat oleh *Certification Authority* dan disepakati oleh *subscriber*;
2.8. Setiap *subscriber* bertanggung jawab atas keamanan kunci pribadi yang dimilikinya dan tidak boleh mengungkapkan kunci pribadi tersebut kepada siapapun yang tidak berhak;
2.9. Kunci pribadi harus disimpan dalam media penyimpanan yang aman;
2.10. Tata Cara Penerbitan Pasangan Kunci dan Sertifikat Elektronik diatur dalam Lampiran I Pedoman ini.

3. Ketentuan Penyebaran Kunci Publik dan Sertifikat Elektronik

3.1. *Certification Authority* melakukan publikasi atas kunci publik dan sertifikat elektronik dengan menggunakan *server* khusus (*repository*) untuk penyebaran sertifikat elektronik yang dapat diakses melalui jaringan komunikasi data DJP;
3.2. *Subscriber* dilarang melakukan penyebaran kunci publik antar individu/ *private dissemination* secara langsung.
3.3. *Certification Authority* bertanggung jawab atas pengoperasian *server* yang digunakan untuk kegiatan penyebaran kunci publik dan sertifikat elektronik;
3.4. Individu atau organisasi yang mengandalkan sertifikat elektronik dalam mempercayai pihak lain atau informasi yang disampaikan pihak lain *(relying party)* dapat mengunduh kunci publik dan sertifikat elektronik dari *server* penyebaran sertifikat elektronik setelah melakukan *login* terlebih dahulu dan menyetujui *Relying Party Agreement;*
3.5. Hak dan kewajiban *relying party* yang akan menggunakan kunci publik dan sertifikat elektronik dituangkan dalam sebuah kesepakatan (*Relying Party Agreement*);
3.6. Format tampilan *Relying Party Agreement* diatur dalam Lampiran V pada Pedoman ini.

4. Ketentuan Penggunaan Pasangan Kunci dan Sertifikat Elektronik

4.1. *Subscriber* hanya boleh menggunakan kunci pribadi dan sertifikat elektronik untuk keperluan yang tepat sesuai dengan kesepakatan/*Subscriber Agreement* pada saat pendaftaran untuk mendapatkan pasangan kunci*;*
4.2. Penggunaan kunci pribadi dan sertifikat elektronik hanya dapat dilakukan setelah keduanya dipublikasikan melalui *server* penyebaran sertifikat elektronik oleh *Certification Authority*;
4.3. Kunci pribadi dan sertifikat elektronik yang masa berlakunya telah habis harus tidak dapat digunakan lagi;
4.4. *Relying party* harus membaca dan menyetujui *Relying Party Agreement* sebelum menggunakan kunci publik dan sertifikat elektronik;
4.5. *Relying party* harus memeriksa status dari kunci publik dan sertifikat elektronik sebelum digunakan, sehingga kunci publik yang dipakai untuk mengenkripsi pesan atau file dan memverifikasi tanda tangan digital adalah kunci yang masih berlaku.

5. Ketentuan Pembatalan Keabsahan serta Penghapusan Sertifikat Elektronik

5.1. Keabsahan sertifikat elektronik dapat dibatalkan sebelum masa berlakunya habis dalam hal:

5.1.1. Pegawai yang menjadi subjek sertifikat elektronik tersebut tidak bekerja lagi di Direktorat Jenderal Pajak;
5.1.2. Wajib Pajak yang menjadi subjek sertifikat elektronik tersebut tidak terdaftar lagi di DJP;
5.1.3. Pihak ketiga yang menjadi subjek sertifikat elektronik tersebut telah berakhir masa kerjasamanya dengan DJP;
5.1.4. Kunci pribadi dari sertifikat elektronik tersebut hilang atau diketahui oleh pihak lain yang tidak berhak.

5.2. Dalam hal *subscriber* mengalami kondisi sebagaimana disebutkan pada angka 5.1.4, maka *subscriber* tersebut berkewajiban untuk mengajukan permohonan pembatalan keabsahan sertifikat elektronik kepada *Certification Authority*;
5.3. Dalam rangka memberikan informasi kepada *relying party* mengenai sertifikat elektronik yang dibatalkan keabsahannya, maka *Certification Authority (CA)* bertanggung jawab untuk membuat Daftar Sertifikat elektronik yang Dibatalkan Keabsahannya (selanjutnya disebut *Certificate Revocation List*/*CRL*) dalam format *certificate revocation list file*;
5.4. *Certification Authority (CA)* menandatangani CRL secara elektronik;
5.5. *Certificate Revocation List (CRL)* paling sedikit harus memuat informasi mengenai:

5.5.1. Algoritma yang digunakan untuk menandatangani CRL;
5.5.2. Tanggal penerbitan CRL;
5.5.3. Periode berlakunya CRL;
5.5.4. Daftar sertifikat elektronik yang dibatalkan keabsahaannya dan tanggal pembatalannya.

5.6. *Certificate Revocation List (CRL)* disebarkan melalui *server* bersama dengan sertifikat elektronik;
5.7. *Certification Authority* bertanggung jawab untuk menghapus sertifikat elektronik yang dibatalkan keabsahannya dari *server* yang digunakan untuk penyebaran sertifikat elektronik;
5.8. *Certification Authority* membuat Berita Acara Pembatalan Keabsahan Sertifikat elektronik sebagai dokumentasi;
5.9. Tata Cara Pembatalan Keabsahan Sertifikat elektronik diatur dalam Lampiran II Pedoman ini.

6. Ketentuan Penerbitan Kembali Pasangan Kunci dan Sertifikat Elektronik

6.1. *Subscriber* dapat mengajukan permohonan penerbitan kembali pasangan kunci dan sertifikat elektronik dalam hal:
6.1.1. Umur penggunaan kunci publik dan sertifikat elektronik telah habis;
6.1.2. Sertifikat elektronik dibatalkan keabsahannya karena kunci pribadi hilang atau diketahui pihak lain;
6.2. *Certification Authority* melakukan penerbitan kembali pasangan kunci berdasarkan permohonan penerbitan kembali dari *subscriber*;
6.3. Tata cara penerbitan kembali pasangan kunci dan sertifikat elektronik mengacu kepada Tata Cara Penerbitan Pasangan Kunci dan Sertifikat Elektronik sebagaimana pada Lampiran I Pedoman ini;
6.4. Dalam rangka memudahkan *relying party* dalam pencarian sertifikat elektronik berdasarkan masa berlakunya, maka *Certification Authority* bertanggung jawab untuk memindahkan sertifikat elektronik yang telah habis masa berlakunya ke direktori khusus sebagai arsip.

7. Ketentuan *Backup* dan *Restore* Sistem Pengelolaan Kunci Kriptografi

7.1. Dalam rangka menjamin kelangsungan layanan kriptografi, maka Kepala Seksi Pengelolaan Intranet dan Internet, Direktorat Teknologi Informasi Perpajakan bertanggung jawab untuk mem*backup* sistem pengelolaan kunci termasuk seluruh kunci publik, sertifikat elektronik, dan *certificate revocation list*;
7.2. Pelaksanaan *backup* dan *restore* pada *server* yang digunakan untuk penyebaran kunci publik, sertifikat elektronik, dan CRL mengacu pada Pedoman *Backup* dan *Restore* Sistem/Data/Informasi.

8. Ketentuan *Cross Certification*

8.1. Direktur Jenderal Pajak dapat membuat suatu perjanjian sertifikasi silang/*cross certification* dengan organisasi lain jika diperlukan dalam rangka menunjang kelancaran transaksi pertukaran data/informasi yang sifatnya rahasia atau sangat rahasia;
8.2. Dengan adanya perjanjian *cross certification* maka *relying party* pada *Public Key Infrastructure* DJP dapat mempercayai sertifikat elektronik dari *Public Key Infrastructure* organisasi lain yang terikat perjanjian tersebut.

9. Pelaporan Pengelolaan Kunci Kriptografi

9.1. Kepala Seksi Pengelolaan Intranet dan Internet, Dit. TIP membuat laporan kegiatan penerbitan, pendistribusian, pembatalan, penghapusan, dan penerbitan kembali sertifikat elektronik;
9.2. Tata Cara Pelaporan Pengelolaan Kunci Kriptografi dijelaskan dalam Lampiran III Pedoman ini.

F. Daftar Istilah:

1. **Kriptografi** adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi. Bentuk pemanfaatan kriptografi dalam keamanan informasi diantaranya adalah enkripsi, penggunaan sertifikat elektronik, penggunaan tanda tangan elektronik, dan mekanisme *hash*;
2. **Enkripsi** adalah suatu proses untuk mengamankan informasi dengan cara mengubahnya menjadi tidak terbaca dengan menggunakan algoritma tertentu;
3. ***Key Management*** adalah suatu ketentuan dalam desain sistem kriptografi yang berhubungan dengan pembuatan, pertukaran, penyimpanan, pengamanan, penggunaan, dan penggantian *key*. *Key management* meliputi desain protokol kriptografi, *key server*, prosedur pengguna, dan protokol lainnya yang relevan;
4. **Dekripsi** adalah proses pembalikkan algoritma yang digunakan dalam enkripsi;
5. **Enkripsi Simetris** adalah metode kriptografi yang menggunakan kunci tunggal untuk proses enkripsi maupun dekripsi;
6. **Enkripsi Asimetris** adalah metode kriptografi yang menggunakan pasangan kunci yang berbeda (publik dan pribadi). Pada metode ini enkripsi dilakukan dengan kunci publik/*public key* dan dekripsi dilakukan dengan kunci pribadi/*private key*;
7. **Enkripsi Hibrid** adalah metode kriptografi di mana data/informasi dilindungi dengan enkripsi simetris sedangkan keamanan pengiriman kunci kriptografi dilakukan dengan enkripsi asimetris;
8. ***Hash*** adalah metode kriptografi berupa prosedur matematis yang mengambil blok data dari pesan/informasi secara acak untuk menghasilkan nilai dengan ukuran yang tetap (nilai *hash*). Nilai ini akan berubah apabila pesan/informasi berubah;
9. **Data/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, 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 memahami;
10. **Data atau Informasi Sensitif** adalah semua data atau informasi yang berdasarkan Kebijakan Pengelolaan Kemanan Informasi DJP diklasifikasikan sebagai data atau informasi yang sangat rahasia atau rahasia;
11. **Pengguna Aset Informasi** adalah Pegawai DJP atau Pihak Ketiga yang menggunakan fasilitas pengolah informasi milik DJP;
12. **Pengirim Data/Informasi** atau Pengirim adalah Pengguna Aset Informasi yang melakukan

pengiriman data/informasi kepada Penerima data/informasi;

13. **Penerima Data/Informasi** atau Penerima adalah Pengguna Aset Informasi yang menjadi penerima data/informasi yang dikirimkan oleh Pengirim data/informasi;
14. **Penyimpan Data/Informasi** atau Penyimpan adalah Pengguna Aset Informasi yang melakukan penyimpanan data/informasi untuk digunakan kembali pada waktu mendatang;
15. **Administrator Sistem** adalah pegawai DJP yang ditunjuk untuk mengelola, melakukan pemeliharaan, dan pengawasan terhadap sistem TIK serta bertanggung jawab terhadap integritas data, efisiensi, dan kinerja sistem TIK;
16. **Pemantau Kemanan Jaringan** adalah Pegawai Direktorat TIP yang ditugaskan untuk memantau keamanan jaringan komunikasi data di DJP;
17. **Pengguna aplikasi** adalah pegawai, wajib pajak, atau pihak ketiga yang memanfaatkan aplikasi milik DJP;
18. **Kunci Kriptografi** adalah sebuah parameter yang terkait dengan algoritma kriptografi. Pihak yang memiliki pengetahuan mengenai parameter ini dapat membalikkan proses algoritma yang dilakukan pada saat enkripsi;
19. **Pasangan Kunci** adalah kunci kriptografi yang digunakan dalam metode enkripsi asimetris, terdiri dari kunci publik dan kunci pribadi;
20. **Kunci Publik** adalah bagian dari kunci berpasangan yang dapat diberikan kepada pihak lain untuk mengenkripsi pesan atau file yang akan dikirim kepada pemilik kunci berpasangan tersebut. Kunci publik juga dapat digunakan untuk memvalidasi tanda tangan digital yang dibuat dengan kunci pribadi pasangannya;
21. **Kunci Pribadi** adalah pasangan dari kunci publik yang digunakan untuk mendekripsi pesan atau file yang dienkripsi dengan kunci publik pasangannya. Kunci pribadi juga dapat digunakan untuk menandatangani pesan atau file secara elektronik (*digital signature*);
22. ***Public Key Infrastructure*** adalah teknologi yang digunakan untuk menyediakan infrastruktur kriptografi dalam bentuk pasangan kunci (publik - pribadi);
23. **Sertifikat Elektronik** adalah sertifikat yang bersifat elektronik yang memuat kunci publik dan identitas yang menunjukan subjek hukum para pihak dalam transaksi elektronik, yang dikeluarkan oleh Certification Authority/Penyelenggara Sertifikasi;
24. ***Digital Signature*** adalah jenis tanda tangan elektronik yang menerapkan teknik kriptografi yang dapat ditempelkan pada pesan/data yang dikirim secara elektronik untuk menunjukkan identitas pengirim pesan dan menjamin bahwa yang mengirimkan pesan itu memang benar-benar orang yang seharusnya;
25. ***Secure Socket Layer (SSL/TLS)*** adalah protokol jaringan yang menerapkan sistem kriptografi dengan pasangan kunci dan sertifikat elektronik untuk mengamankan aplikasi berbasis web;
26. ***File Transfer Protocol*** adalah protokol jaringan yang digunakan untuk pertukaran data atau informasi melalui jaringan intranet atau internet;
27. ***Secure File Transfer Protocol*** adalah protokol jaringan yang digunakan untuk pertukaran data atau informasi melalui jaringan intranet atau internet yang telah menerapkan enkripsi untuk melindungi keamanannya;
28. ***Secure Shell (SSH)*** adalah protokol jaringan berbasis Unix yang digunakan untuk melakukan akses jarak jauh ke komputer lain dalam jaringan secara aman. Koneksi antara *server* dengan *client* diotentikasi dengan *digital certificate* dan password, kemudian pertukaran data antara *server* dan *client* dilindungi dengan enkripsi asimetris;
29. ***Subscriber*** adalah orang atau perangkat lunak yang menjadi subjek dari kunci publik dan sertifikat elektronik;
30. ***Relying Party*** adalah individu atau organisasi yang mengandalkan kunci publik atau sertifikat elektronik sebagai dasar untuk mempercayai identitas seseorang atau suatu data/informasi yang disampaikan oleh pihak lain;
31. ***Certification Authority* DJP** adalah pejabat pada Direktorat Teknologi Informasi Perpajakan yang memiliki peran untuk mensertifikasi identitas dari setiap *subscriber* dalam jaringan komunikasi data DJP supaya dapat dikenali;
32. ***Registration Authority* DJP** adalah Pegawai pada Seksi Pengelolaan Intranet dan Internet, Direktorat Teknologi Informasi Perpajakan yang bertugas melakukan otentikasi terhadap setiap *subscriber*, menerbitkan pasangan kunci, membuat daftar sertifikat elektronik yang dibatalkan keabsahannya, dan tugas lainnya selain menandatangani sertifikat elektronik;
33. ***Subscriber Agreement*** adalah perjanjian yang berisi syarat dan ketentuan yang harus dibaca dan disetujui oleh setiap *subscriber* sebelum memanfaatkan kunci pribadi dan sertifikat elektronik untuk dekripsi, tanda tangan digital, atau keperluan lainnya;
34. ***Relying Party Agreement*** adalah perjanjian yang berisi tentang syarat dan ketentuan yang harus dibaca dan disetujui oleh setiap *relying party* sebelum memanfaatkan kunci publik dan sertifikat elektronik untuk enkripsi, verifikasi tanda tangan digital, dan keperluan lainnya;
35. ***Cross Certification*** adalah kesepakatan antara dua atau lebih organisasi untuk saling mempercayai sertifikat elektronik yang diterbitkan oleh masing-masing organisasi tersebut.
36. ***Key Server*** adalah tempat penyimpanan (*repository*) sertifikat elektronik yang digunakan untuk mempublikasikannya;
37. ***Electronic Mail atau e-mail*** adalah fasilitas surat menyurat melalui jalur komunikasi elektronik baik Internet maupun Intranet. Setiap pengguna yang memiliki alamat e-mail dapat saling berkirim surat layaknya menggunakan kertas melalui kantor pos.
38. ***Backup*** adalah proses pembuatan salinan sistem/data/informasi yang berada dalam satu atau beberapa komputer, ke dalam suatu media eksternal seperti *tape*, *CD*, *DVD*, *hard disk*, atau media eksternal lainnya sebagai cadangan dari sistem/data/informasi aslinya mana kala terjadi suatu kerusakan, kesalahan operasional atau sebab yang lain.
39. **Fasilitas Pengolah Informasi** adalah sistem informasi termasuk perangkat lunak dan perangkat keras milik Direktorat Jenderal Pajak yang dimanfaatkan untuk mengolah data/informasi dalam rangka menjalankan tugas dan fungsinya.
40. ***Service Desk* TIK** adalah unit kerja TIK DJP yang bertindak sebagai *Single Point of Contact* (SPOC) atau gerbang layanan TIK terdepan yang memiliki peran strategis dalam meningkatkan kepuasan pengguna layanan TIK. *Service Desk* TIK bukan diposisikan sebagai tenaga teknis semata, namun lebih luas lagi harus bertindak sebagai unit pelayanan TIK bagi pengguna;

41. ***Removable Media*** adalah media penyimpan data elektronik yang dapat dipindahkan dan tidak terpasang secara permanen pada komputer, misal *compact disks*, DVD *disk*, *memory stick*, USB *drive*, *floppy disk*, dan sebagainya.

LAMPIRAN I
Pedoman Enkripsi dan *Key Management*

Tata Cara Penerbitan serta Penyebaran Pasangan Kunci dan Sertifikat Elektronik

A. Deskripsi :

Prosedur operasi ini menguraikan proses penerbitan serta penyebaran pasangan kunci (publik-pribadi) dan sertifikat elektronik untuk *subscriber* (pegawai DJP, wajib pajak, dan pihak ketiga).

B. Dasar Hukum :

Peraturan Direktur Jenderal Pajak Nomor PER-41/PJ/2010 tentang Kebijakan Pengelolaan Keamanan Informasi Direktorat Jendral Pajak.

C. Surat Edaran Terkait :

-

D. Pihak yang Terkait :

1. Kepala Seksi Pengelolaan Intranet dan Internet Direktorat TIP;
2. Pelaksana Seksi Pengelolaan Intranet dan Internet Direktorat TIP;
3. *Service Desk TIK*;
4. *Subscriber* (Pegawai DJP, Wajib Pajak, Pihak Ketiga).

E. Formulir yang Digunakan :

Formulir Permohonan Penerbitan Sertifikat elektronik

F. Dokumen yang Dihasilkan :

-

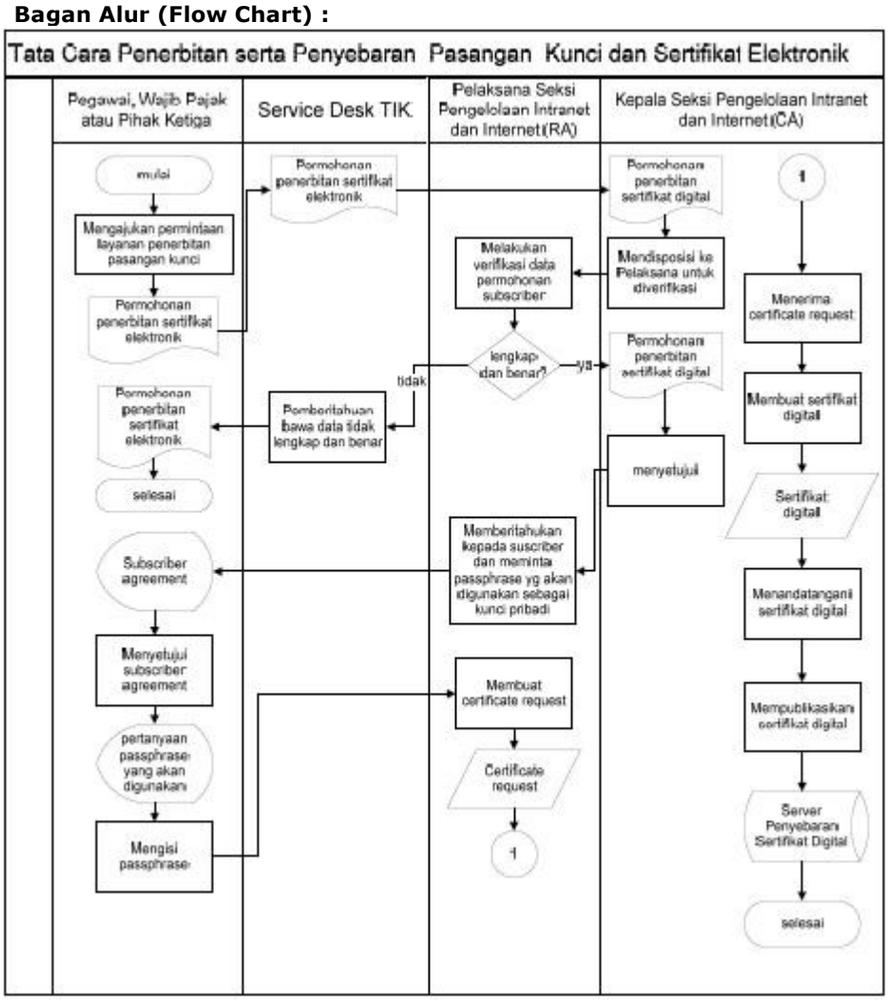
G. Prosedur Kerja :

1. *Subscriber* mengajukan permintaan layanan penerbitan sertifikat elektronik kepada *Service Desk TIK*;
2. *Service Desk TIK* mengeskalasi permohonan penerbitan sertifikat elektronik ke Seksi Pengelolaan Intranet dan Internet, Direktorat Teknologi Informasi Perpajakan;
3. Kepala Seksi Pengelolaan Intranet dan Internet menerima formulir permohonan penerbitan sertifikat elektronik dan mendisposisikan ke pelaksana untuk dilakukan verifikasi atas kelengkapan dan kebenaran data yang disampaikan;
4. Pelaksana Seksi Pengelolaan Intranet dan Internet melakukan verifikasi terhadap data yang disampaikan dalam Permohonan Penerbitan Sertifikat elektronik. Apabila Permohonan tersebut telah benar dan lengkap maka diberikan tanda berupa stempel lengkap dan mengirimkan ke Kepala Seksi untuk disetujui, dan apabila data yang disampaikan tidak benar atau tidak lengkap maka akan diberikan tanda tidak lengkap dan dikembalikan kepada *subscriber*;
5. Apabila permohonan penerbitan sertifikat elektronik disetujui oleh Kepala Seksi Pengelolaan Intranet dan Internet maka Pelaksana mengirimkan pemberitahuan kepada *subscriber* melalui *e-mail* disertai *link* yang akan mengarahkan subscriber ke Aplikasi Pengelolaan Kunci Kriptografi milik DJP;
6. *Subscriber* mengisikan *passphrase* yang akan digunakan sebagai kunci pribadi;
7. Pelaksana Seksi Pengelolaan Intranet dan Internet membuat *certificate request file* dari setiap *susbcriber* yang telah mengisi *passphrase*;
8. Pelaksana Seksi Pengelolaan Intranet dan Internet mengirimkan *certificate request file* kepada Kepala Seksi Intranet dan Internet untuk dibuatkan sertifikat elektronik;
9. Kepala Seksi Pengelolaan Intranet dan Internet memproses *certificate request file* menjadi sertifikat elektronik dan menandatanganinya secara digital dengan kunci *Certificate Authority* DJP;
10. Kepala Seksi Pengelolaan Intranet dan Internet mempublikasikan sertifikat elektronik dari setiap *subscriber* melalui *server* penyebaran sertifikat elektronik yang dapat diakses melalui jaringan komunikasi data DJP ;
11. Proses penerbitan pasangan sertifikat elektronik selesai.

Jangka Waktu Penyelesaian :

3 hari kerja semenjak permohonan penerbitan pasangan kunci publik-pribadi dan sertifikat elektronik disampaikan oleh *subscriber* secara lengkap.

H. Bagan Alur (Flow Chart) :



LAMPIRAN II
Pedoman Enkripsi dan *Key Management*

Tata Cara Pembatalan Keabsahan Sertifikat Elektronik

A. Deskripsi :

Prosedur operasi ini menguraikan proses pembatalan keabsahan kunci publik dan sertifikat elektronik, dengan tujuan untuk memastikan bahwa pembatalan keabsahan kunci publik dan sertifikat elektronik dilaksanakan secara konsisten.

B. Dasar Hukum :

Peraturan Direktur Jenderal Pajak Nomor PER-41/PJ/2010 tentang Kebijakan Pengelolaan Keamanan Informasi Direktorat Jendral Pajak.

C. Surat Edaran Terkait :

-

D. Pihak yang Terkait :

1. Kepala Seksi Pengelolaan Intranet dan Internet, Direktorat Teknologi Informasi Perpajakan;
2. Pelaksana Seksi Pengelolaan Intranet dan Internet, Direktorat Teknologi Informasi Perpajakan;
3. *Subscriber* (Pegawai DJP, Wajib Pajak, Pihak ketiga).

E. Formulir yang Digunakan :

Formulir Permohonan Pembatalan Keabsahan Sertifikat Elektronik

F. Dokumen yang Dihasilkan :

Berita Acara Pembatalan Keabsahan Kunci Publik dan Sertifikat Elektronik

G. Prosedur Kerja :

1. Proses dapat dimulai dari salah satu kondisi berikut :
   1.1. Seksi Pengelolaan Intranet dan Internet mengumpulkan informasi mengenai hal-hal berikut ini:
      1.1.1. Pegawai DJP sebagai pemegang sertifikat elektronik berhenti bekerja;
      1.1.2. Wajib pajak tidak terdaftar lagi di DJP;
      1.1.3. Pihak ketiga telah habis masa kerja samanya dengan DJP, atau
      1.1.4. Informasi mengenai bocornya kunci pribadi *subscriber* kepada pihak lain.

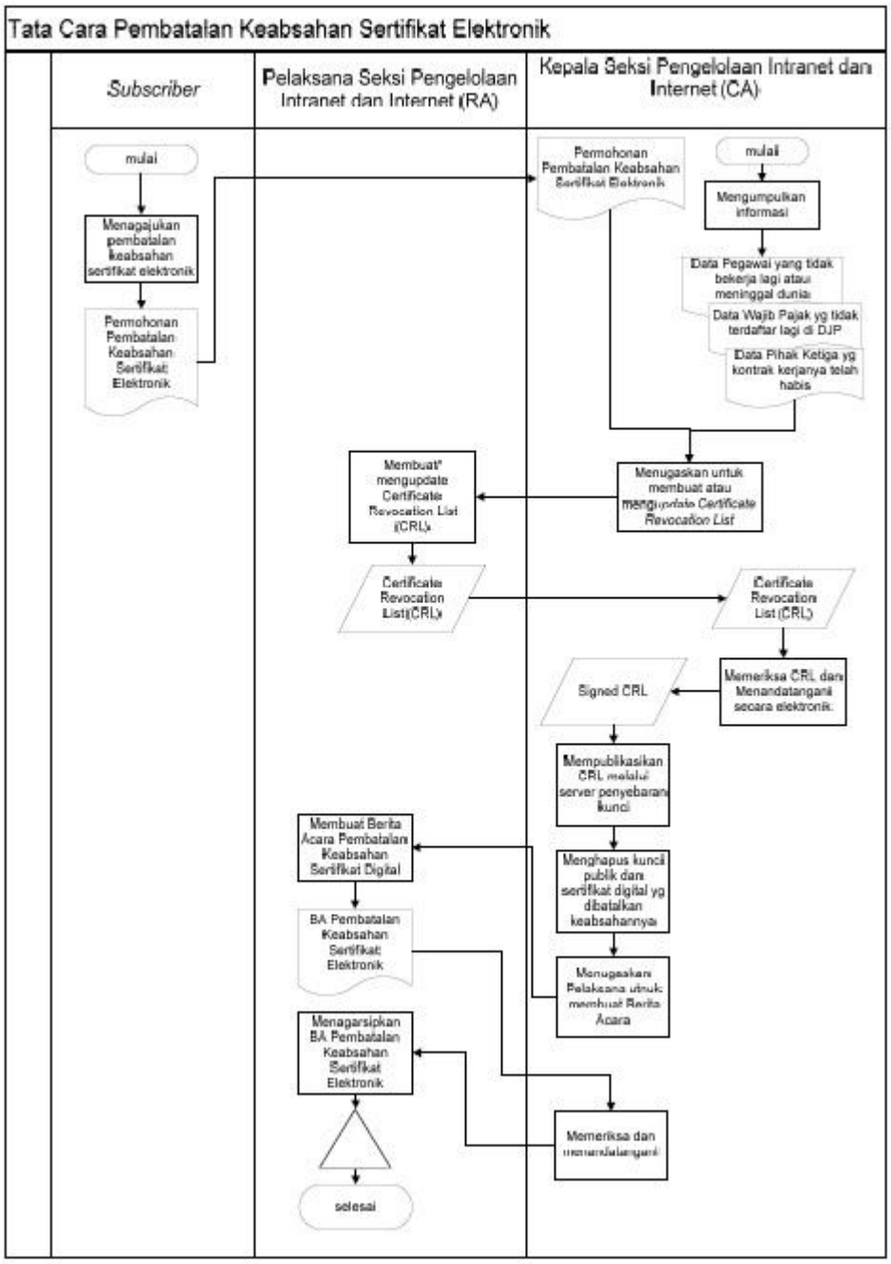
   1.2. *Subscriber* mengajukan permohonan pembatalan keabsahan *kunci publik* dan *sertifikat elektronik* kepada Kepala Seksi Pengelolaan Intranet dan Internet, karena kunci pribadinya bocor kepada pihak lainnya yang tidak berhak.

2. Kepala Seksi Pengelolaan Intranet dan Internet menugaskan Pelaksana untuk membuat atau meng*update Certificate Revocation List;*
3. Pelaksana Seksi Pengelolaan Intranet dan Internet membuat atau meng*update Certificate Revocation List* (CRL), kemudian mengirimkannya kepada Kepala Seksi Pengelolaan Intranet dan Internet.
4. Kepala Seksi Pengelolaan Intranet dan Internet memeriksa kemudian menandatangani CRL secara digital.
5. Kepala Seksi Pengelolaan Intranet dan Internet mempublikasikan CRL melalui *repository/server* penyebaran kunci.
6. Kepala Seksi Pengelolaan Intranet dan Internet menghapus sertifikat elektronik yang telah dibatalkan keabsahannya dari *server* penyebaran kunci.
7. Kepala Seksi Pengelolaan Intranet dan Internet menugaskan pelaksana untuk membuat Berita Acara Pembatalan Keabsahan Sertifikat Elektronik.
8. Pelaksana Seksi Pengelolaan Intranet dan Internet membuat Berita Acara Pembatalan Keabsahan Sertifikat Elektronik.
9. Kepala Seksi Pengelolaan Intranet dan Internet menandatangani Berita Acara Pembatalan Keabsahan Sertifikat Elektronik kemudian menugaskan Pelaksana Seksi Pengelolaan Intranet dan Internet untuk mengarsipkan Berita Acara tersebut.
10. Pelaksana Seksi Pengelolaan Intranet dan Internet mengarsipkan Berita Acara Pembatalan Sertifikat elektronik berdasarkan nomor berita acara.
11. Proses pembatalan keabsahan sertifikat elektronik selesai.

Jangka Waktu Penyelesaian :

2 hari kerja semenjak kondisi yang menyebabkan pembatalan keabsahan sertifikat digital terjadi atau semenjak permohonan pembatalan sertifikat digital disampaikan oleh *subscriber* secara lengkap.

H. Bagan Alur (*Flow Chart*) :


Tata Cara Pembatalan Keabsahan Sertifikat Elektronik
Subscriber
Pelaksana Seksi Pengelolaan Intranet dan Internet (RA)
Kepala Seksi Pengelolaan Intranet dan Internet (CA)
mulai
Menagajukan pembatalan keabsahan sertifikat elektronik
Permohonan Pembatalan Keabsahan Sertifikat Elektronik
Permohonan Pembatalan Keabsahan Sertifikat Elektronik
mulai
Mengumpulkan informasi
Data Pegawai yang tidak bekerja lagi atau meninggal dunia
Data Wajib Pajak yg tidak terdaftar lagi di DJP
Data Pihak Ketiga yg kontrak kerjanya telah habis
Membuat/ mengupdate Certificate Revocation List (CRL)
Menugaskan untuk membuat atau mengupdate Certificate Revocation List
Certificate Revocation List(CRL)
Certificate Revocation List (CRL)
Signed CRL
Memeriksa CRL dan Menandatangani secara elektronik
Mempublikasikan CRL melalui server penyebaran kunci
Membuat Berita Acara Pembatalan Keabsahan Sertifikat Digital
Menghapus kunci publik dari sertifikat digital yg dibatalkan keabsahannya
BA Pembatalan Keabsahan Sertifikat Elektronik
Menugaskan Pelaksana untuk membuat Berita Acara
Menagarsipkan BA Pembatalan Keabsahan Sertifikat Elektronik
Memeriksa dan menandatangani
selesai

LAMPIRAN III
Pedoman Enkripsi dan *Key Management*

Tata Cara Pelaporan Kegiatan Pengelolaan Kunci Kriptografi

A. Deskripsi :

Prosedur operasi ini menguraikan proses pelaporan hasil pemantauan penerapan kriptografi untuk melindungi keamanan sistem dan jaringan komunikasi data.

B. Dasar Hukum :

Peraturan Direktur Jenderal Pajak Nomor PER-41/PJ/2010 tentang Kebijakan Pengelolaan Keamanan Informasi Direktorat Jendral Pajak.

C. Surat Edaran Terkait :

-

D. Pihak yang Terkait :

a. Direktur Teknologi Informasi Perpajakan
b. Kepala Subdit Pendukung Operasional
c. Kepala Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data
d. Pelaksana Seksi Pemantauan Keamanan Sistem dan jaringan Komunikasi Data

E. Formulir yang Digunakan :

-

F. Dokumen yang Dihasilkan :

Laporan Pengelolaan Kunci Kriptografi

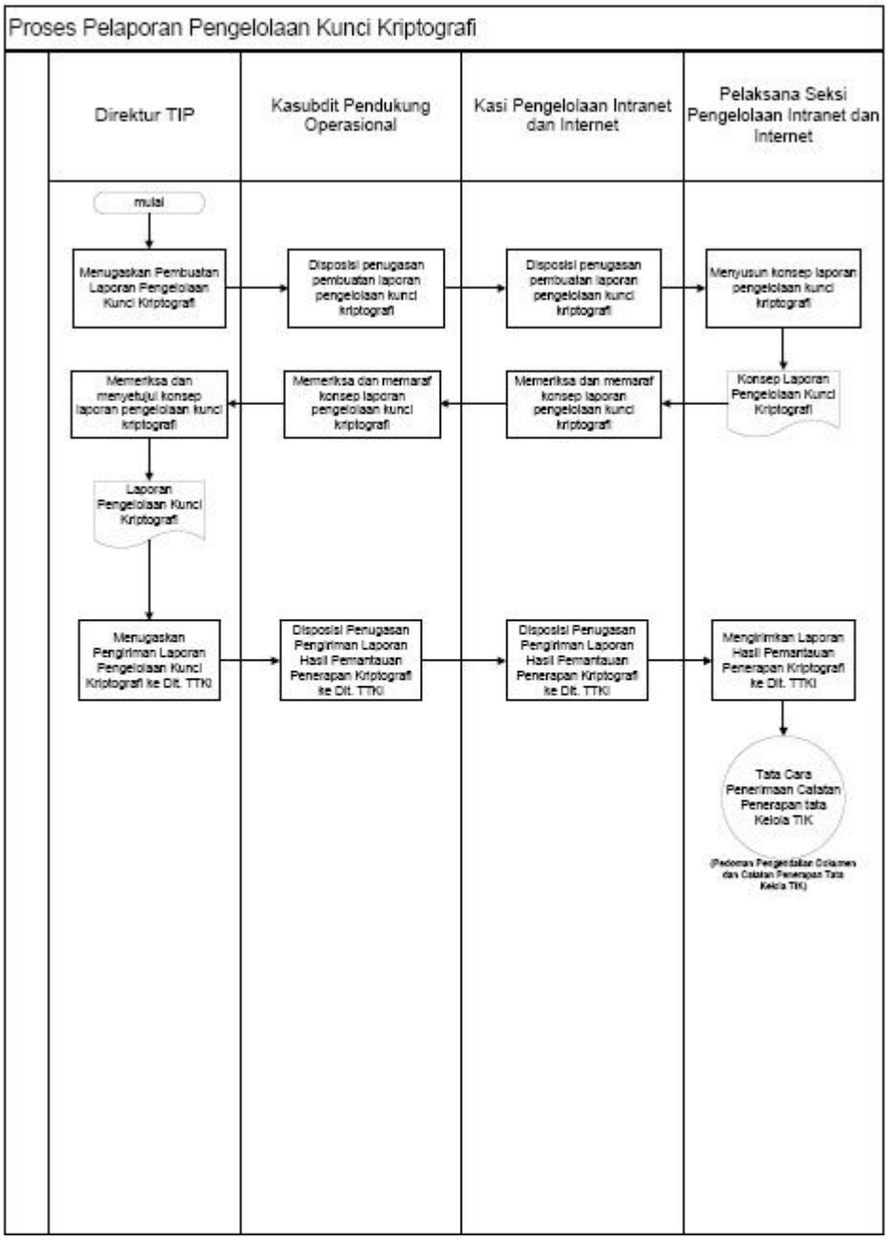
G. Prosedur Kerja :

1. Kepala Subdit Pendukung Operasional menugaskan Kasi Pengelolaan Intranet dan Internet untuk melakukan penyusunan Laporan Pengelolaan Kunci Kriptografi,
2. Kepala Seksi Pengelolaan Intranet dan Internet mendisposisikan penugasan kepada Pelaksana Seksi Pengelolaan Intranet dan Internet,
3. Pelaksana Seksi Pengelolaan Intranet dan Internet mengumpulkan data pengelolaan kunci dari sistem pengelolaan kunci kriptografi milik DJP,
4. Pelaksana Seksi Pengelolaan Intranet dan Internet menyusun konsep Laporan Pengelolaan Kunci Kriptografi,
5. Kepala Seksi Pengelolaan Intranet dan Internet memeriksa konsep Laporan Pengelolaan Kunci Kriptografi, kemudian membubuhkan paraf ,
6. Kepala Subdit Pendukung Operasional memeriksa konsep Laporan Pengelolaan Kunci Kriptografi, kemudian membubuhkan paraf,
7. Direktur TIP memeriksa Laporan Pengelolaan Kunci Kriptografi, kemudian menandatanganinya
8. Direktur TIP menugaskan Subdit Pendukung Operasional untuk mengirimkan Laporan Pengelolaan Kunci Kriptografi kepada Direktorat TTKI,
9. Kasubdit Pendukung Operasional mendisposisikan tugas pengiriman kepada Kasi Pengelolaan Intranet dan Internet,
10. Kasi Pengelolaan Intranet dan Internet mendisposisikan tugas pengiriman Laporan Pengelolaan Kunci Kriptografi kepada Pelaksana Seksi Pengelolaan Intranet dan Internet,
11. Pelaksana Seksi Pengelolaan Intranet dan Internet mengirimkan Laporan Pengelolaan Kunci Kriptografi kepada Direktorat TIP,
12. Proses dilanjutkan ke penerimaan dokumen dan/atau catatan penerimaan dokumen penerapan tata kelola TIK dengan mengacu pada Pedoman Pengendalian Dokumen dan/atau Catatan Penerapan Tata Kelola TIK.

Jangka Waktu Penyelesaian :

5 hari kerja sejak berakhirnya bulan pelaporan.

H. Bagan Alur (*Flow Chart*) :



LAMPIRAN IV
Pedoman Enkripsi dan *Key Management*

Subscriber Agreement

1. Deskripsi

Perjanjian pemohon (*subscriber agreement*) ini berisi syarat dan ketentuan yang harus dibaca dan disetujui oleh setiap subscriber sebelum memanfaatkan *kunci pribadi* dan sertifikat elektronik untuk dekripsi, tanda tangan digital, dan keperluan lainnya.

2. Definisi

Semua istilah dan singkatan dalam dokumen ini memiliki pengertian yang sama sebagaimana tertuang dalam Pedoman Enkripsi dan *Key Management*.

3. Syarat dan Ketentuan

3.1. Dengan menggunakan layanan kriptografi yang disediakan oleh Direktorat Jenderal Pajak, berarti anda (*subscriber)* telah menyetujui semua syarat dan kondisi sebagaimana tertuang dalam dokumen ini.

3.2. Kewajiban anda *(subscriber)* sebelum menggunakan *kunci pribadi* dan sertifikat elektronik:

3.2.1. Menjamin bahwa semua informasi yang disampaikan pada saat pendaftaran adalah benar.
3.2.2. Membaca ketentuan dalam Pedoman Enkripsi dan *Key Management*.
3.2.3. Memeriksa kembali status sertifikat elektronik pada *Certificate Revocation List* (CRL).
3.2.4. Mengetahui bahwa kunci pribadi dan sertifikat elektronik yang disediakan oleh *Certification Authority* Direktorat Jenderal Pajak tidak diperkenankan untuk penggunaan di luar pekerjaan, pelaksanaan hak dan kewajiban perpajakan, dan pelaksanaan kerja sama.

3.3. Kewajiban anda *(subscriber)* dalam penggunaan kunci pribadi dan sertifikat elektronik:

3.3.1. Menjaga kerahasiaan kunci pribadi yang digunakan, dan melakukan upaya yang memungkinkan untuk menghindarkan kunci pribadi dari kehilangan, pengungkapan kepada pihak lain yang tidak semestinya, modifikasi, dan penggunaan lainnya yang tidak terotorisasi.
3.3.2. Menghentikan penggunaan kunci pribadi dan sertifikat elektronik apabila sertifikat elektronik yang dimiliki telah dinyatakan batal keabsahannya oleh *Certification Authority* (CA).
3.3.3. Mengajukan permohonan pembatalan keabsahan kepada CA atas sertifikat yang kunci pribadinya hilang, atau diketahui oleh orang lain yang tidak semestinya.
3.3.4. Memberikan hak kepada CA untuk membatalkan keabsahan sertifikat elektronik apabila terjadi kondisi yang mengharuskannya sebagaimana diatur dalam Pedoman Enkripsi dan *Key Management*.
3.3.5. Menghentikan penggunaan kunci pribadi dan sertifikat elektronik pada saat masa berlakunya berakhir.
3.3.6. Mengetahui bahwa CA telah memberi peringatan tentang kemungkinan pencurian kunci pribadi oleh pihak lain baik yang dapat terdeteksi ataupun tidak dapat terdeteksi.
3.3.7. Anda bersedia menanggung setiap dampak hukum yang diakibatkan oleh kesalahan/ kelalaian dalam penggunaan kunci pribadi dan sertifikat elektronik.

LAMPIRAN V
Pedoman Enkripsi dan *Key Management*

Relying Party Agreement

1. Deskripsi

Perjanjian *relying party* ini berisi syarat dan ketentuan yang harus dibaca dan disetujui oleh *setiap relying party* sebelum memanfaatkan kunci publik dan sertifikat elektronik untuk enkripsi, verifikasi tanda tangan digital, dan keperluan lainnya.

2. Definisi

Semua istilah dan singkatan dalam dokumen ini memiliki pengertian yang sama sebagaimana tertuang dalam Pedoman Enkripsi dan *Key Management*.

3. Syarat dan Ketentuan

3.1. Dengan menggunakan layanan kriptografi yang disediakan oleh Direktorat Jenderal Pajak, berarti anda (*relying party)* telah menyetujui semua syarat dan ketentuan sebagaimana tertuang dalam dokumen ini.
3.2. Kewajiban anda *(relying party)* sebelum menggunakan kunci publik dan sertifikat elektronik:

3.1.1. Membaca ketentuan dalam Pedoman Enkripsi dan *Key Management*.
3.1.2. Memeriksa kembali status kunci publik dan sertifikat elektronik pada *Certificate Revocation List*.
3.1.3. Menggunakan kunci publik dan sertifikat elektronik yang statusnya masih berlaku.
3.1.4. Menghapus serta tidak menggunakan kunci publik dan sertifikat elektronik yang masuk dalam *Certificate Revocation List*.
3.1.5. Mengetahui bahwa kunci publik dan sertifikat elektronik yang disediakan oleh *Certification Authority* (CA) Direktorat Jenderal Pajak tidak diperkenankan untuk digunakan di luar pekerjaan, pelaksanaan hak dan kewajiban perpajakan, atau pelaksanaan kerja sama berdasar perjanjian/kontrak.

4. Ganti Rugi dan Tuntutan Hukum

Anda (*relying party*) bersedia menanggung semua kerugian atau gugatan hukum dari pihak lain yang timbul sebagai akibat dari kelalaian anda dalam melaksanakan setiap kewajiban sebagai *relying party* sebagaimana yang tertera dalam dokumen ini.

LAMPIRAN VI
Pedoman Enkripsi dan *Key Management*

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PAJAK
Gedung B Lantai 4
Jalan Gatot Subroto Kav. 40-42
Jakarta 12190
Website : http://www.pajak.go.id
Telepon 021.52904830
Faksimile 021.5272723

Formulir Permohonan Penerbitan Sertifikat Elektronik
No:.....

Data Pemohon		
Nama	:	.....(1)
Nomor Identitas	:	..... (2)
Nama Organisasi	:	..... (3)
Jabatan	:	..... (4)
Nomor Telepon (Kantor/HP)	:	..... /..... (5)
Alamat *e-mail*	:	.....(6)

Fungsi Sertifikat Elektronik (7)

Fungsi yang dibutuhkan : ☐ Enkripsi ☐ *Digital Signature* ☐ Otentikasi
☐ Lainnya, sebutkan .....

Jenis Permohonan (8)

☐ Penerbitan Pertama Kali ☐ Penerbitan Kembali

Keterangan: (9)
.....

Surat Pernyataan

Pernyataan:
Dengan menandatangani formulir ini,

1. Saya telah memahami dan akan mematuhi kebijakan Keamanan Informasi yang berlaku dalam penggunaan pasangan kunci dan sertifikat elektronik yang diterbitkan oleh *Certification Authority* DJP.
2. Apabila dalam penggunaan pasangan kunci dan sertifikat elektronik ini saya melakukan tindakan yang melanggar kebijakan atau peraturan yang berlaku, saya bertanggung jawab sepenuhnya dan bersedia untuk menanggung segala kerugian yang timbul atau konsekuensi lainnya.

.....,.....(10)
Pemohon,

( )(11)

Persetujuan

Menyetujui,
Certification Authority DJP

( ) (12)
NIP..... (13)

Petunjuk Pengisian
Formulir Permohonan Penerbitan Sertifikat Elektronik

(1) Diisi dengan nama pemohon;
(2) Diisi dengan nomor identitas pemohon misalnya untuk pegawai berupaNIP, untuk Wajib Pajak berupa NPWP, dan untuk pihak ketiga berupa nomor KTP;
(3) Diisi dengan nama organisasi;
(4) Diisi dengan jabatan pemohon dalam organisasi;
(5) Diisi dengan nomor telepon yang dapat dihubungi;
(6) Diisi dengan alamat *e-mail*;
(7) Beri tanda pada fungsi sertifikat elektronik yang dibutuhkan;
(8) Beri tanda pada jenis permohonan yang diajukan;
(9) Hanya diisi jika jenis permohonan adalah penerbitan kembali sertifikat elektronik. Diisi dengan keterangan mengenai dasar penerbitan kembali sertifikat elektronik;
(10) Diisi dengan tempat dan tanggal pengajuan permohonan;
(11) Diisi dengan nama jelas dari pemohon;
(12) Diisi dengan nama pejabat pada Direktorat TIP yang diberikan kewenangan sebagai *Certification Authority* DJP;
(13) Diisi dengan NIP pejabat pada Direktorat TIP yang diberikan kewenangan sebagai *Certification Authority* DJP;

LAMPIRAN VII
Pedoman Enkripsi dan *Key Management*

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PAJAK

Gedung B Lantai 4
Jalan Gatot Subroto Kav. 40-42
Jakarta 12190
Website : http://www.pajak.go.id

Telepon 021.52904830
Faksimile 021.5272723

Formulir Permohonan Pembatalan Keabsahan Sertifikat Elektronik
No:.....

Data Pemohon		
Nama	:	.....(1)
Nomor Identitas	:	..... (2)
Nama Organisasi	:	..... (3)
Jabatan	:	..... (4)
Nomor Telepon (Kantor/HP)	:	..... /..... (5)
Alamat *e-mail*	:	.....(6)
Data Sertifikat Elektronik		
Nomor Seri Sertifikat	:	..... (7)
elektronik	:	..... (8)
Subjek Sertifikasi	:	..... (9)
Subject Key Identifier		
Alasan Permohonan (10)		
☐ Kunci pribadi diketahui oleh pihak lain yang tidak berhak		
☐ Kunci pribadi hilang atau lupa		
Surat Pernyataan		
Pernyataan: Dengan menandatangani formulir ini, 1. Saya menyatakan bahwa informasi dalam Surat Permohonan ini adalah informasi yang sesungguhnya; 2. Apabila di kemudian hari diketahui bawa informasi yang saya sampaikan adalah tidak benar, maka saya bertanggung jawab sepenuhnya dan bersedia untuk menanggung segala kerugian yang timbul atau konsekuensi lainnya. .....,.....(11) Pemohon, ( )(12)		
Persetujuan		
Menyetujui, *Certification Authority* DJP ( ) (13) NIP..... (14)		

Petunjuk Pengisian
Formulir Permohonan Pembatalan Keabsahan Sertifikat Elektronik

(1) Diisi dengan nama pemohon;
(2) Diisi dengan nomor identitas pemohon misalnya untuk pegawai berupa NIP, untuk Wajib Pajak berupa NPWP, dan untuk pihak ketiga berupa nomor KTP;
(3) Diisi dengan nama organisasi;
(4) Diisi dengan jabatan pemohon dalam organisasi;
(5) Diisi dengan nomor telepon yang dapat dihubungi;
(6) Diisi dengan alamat e-mail;
(7) Diisi dengan nomor seri sertifikat elektronik (lihat tab *details* pada sertifikat elektronik);
(8) Diisi dengan nama subjek yang disertifikasi (lihat tab *details* pada sertifikat elektronik);
(9) Diisi dengan *subject key identifier* (lihat tab *details* pada sertifikat elektronik);
(10) Pilih alasan yang mendasari permohonan pembatalan keabsahan sertifikat elektronik;
(12) Diisi dengan nama jelas dari pemohon;
(13) Diisi dengan nama pejabat pada Direktorat TIP yang diberikan kewenangan sebagai *Certification Authority* DJP;
(14) Diisi dengan NIP pejabat pada Direktorat TIP yang diberikan kewenangan sebagai *Certification Authority* DJP;

LAMPIRAN VIII
Pedoman Enkripsi dan *Key Management*

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PAJAK

Jalan Jend. Gatot Subroto Kav. 40-42
Jakarta 12190
Kode Pos 124
Website : http://www.pajak.go.id

Telepon 5250208-5251609
5262880
Faksimile 584792

Berita Acara Pembatalan Keabsahan Sertifikat Elektronik
Nomor: BA-...../...../..... (1)

Berdasarkan hal-hal yang dapat mendasari pembatalan keabsahan sertifikat elektronik berikut:

Kondisi: (2)

☐ Pegawai DJP telah berhenti bekerja
☐ Wajib pajak tidak terdaftar lagi di DJP
☐ Pihak ketiga telah habis masa kerja samanya dengan DJP
☐ Kunci pribadi *subscriber* diketahui oleh pihak lain

Sumber Informasi : (3)

☐ Permohonan dari *subscriber*
☐ Masterfile Wajib Pajak
☐ Sumber lain, sebutkan .....
☐ Informasi kepegawaian
☐ Dokumen Kontrak pihak ketiga

sesuai dengan ketentuan pada Pedoman Enkripsi dan *Key Management*, maka pada hari ini .....(4)....., tanggal ..... (5)..... dilakukan pembatalan keabsahan atas sertifikat elektronik dibawah ini:

Nama subjek/*subscriber* : ..... (6)
Nomor Identitas : ..... (7)
Nomor seri sertifikat elektronik : ..... (8)
Subject key identifier : ..... (9)

Certification Authority DJP

.....(10)
NIP.....(11)

Petunjuk Pengisian Formulir
Berita Acara Pembatalan Keabsahan Sertifikat Elektronik

(1) Diisi dengan nomor Berita Acara sesuai aturan penomoran surat pada unit kerja
(2) Pilih alasan yang mendasari pembatalan keabsahan sertifikat elektronik;
(3) Pilih sumber informasi yang menjadi dasar pembatalan sertifikat elektronik atau sebutkan sumber informasi yang sesuai;
(4) Diisi dengan hari pembatalan keabsahan sertifikat elektronik;
(5) Diisi dengan tanggal, bulan, dan tahun pembatalan keabsahan sertifikat elektronik;
(6) Diisi dengan nama subjek/ *subscriber* dari sertifikat yang dibatalkan keabsahannya;
(7) Diisi dengan nomor identitas subjek dari sertifikat elektronik yang dibatalkna keabsahannya;
(8) Diisi dengan nomor seri dari sertifikat elektronik yang dibatalkan keabsahannya (lihat tab *details* pada sertifikat elektronik);
(9) Diisi dengan kode *subject key identifier* (lihat tab *details* pada sertifikat elektronik):
(10) Diisi dengan nama pejabat pada Direktorat TIP yang memegang fungsi *Certification Authority* DJP;
(11) Diisi dengan NIP pejabat pada Direktorat TIP yang memegang fungsi *Certification Authority* DJP.

LAMPIRAN IX
Pedoman Enkripsi dan *Key Management*

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PAJAK
DIREKTORAT TEKNOLOGI INFORMASI PERPAJAKAN

Jalan Jend. Gatot Subroto 40-42
Jakarta 12190
Kode Pos 124
Website : http://www.pajak.go.id

Telepon 5250208-
5251609
5262880
Faksimile 584792

Laporan Pengelolaan Kunci Kriptografi
Bulan .....(1) Tahun .....(2)
Nomor : .....(3)

No	Kegiatan	Jumlah
1	Menerima Permintaan Penerbitan Pasangan Kunci dan Sertifikat Elektronik	
	a. Pegawai DJP	(4)
	b. Wajib Pajak	
	c. Pihak Ketiga	
	Total	
2	Penerbitan Pasangan Kunci dan Sertifikat Elektronik	
	a. Aplikasi	(5)
	b. Pegawai DJP	
	c. Wajib Pajak	
	d. Pihak Ketiga	
	Total	
3	Menerima Permintaan Pembatalan Keabsahan Sertifikat Elektronik	
	a. Aplikasi	(6)
	b. Pegawai DJP	
	c. Wajib Pajak	
	d. Pihak Ketiga	
	Total	
4	Pembatalan Keabsahan Sertifikat Elektronik	
	a. Aplikasi	(7)
	b. Pegawai DJP	
	c. Wajib Pajak	
	d. Pihak Ketiga	
	Total	
5	Penerbitan Kembali Pasangan Kunci dan Seritifkat Elektronik	
	a. Aplikasi	(8)
	b. Pegawai DJP	
	c. Wajib Pajak	
	d. Pihak Ketiga	
	Total	

Disiapkan oleh,
Kepala Seksi Pengelolaan Internet dan Internet

<.....(9).....>
NIP.....(10).....

Mengetahui,
Direktur Teknologi Informasi Perpajakan

<.....(11).....>
NIP.....(12).....

Menyetujui,
Kepala Subdit Pendukung Operasional

<.....(13).....>
NIP.....(14).....

I. Daftar Permohonan Penerbitan Pasangan Kunci dan Sertifikat Elektronik
Bulan .....(15) Tahun .....(16)

No	No. Surat Permohonan	Nama Subjek	Organisasi	Tanggal	Keterangan
1	2	3	4	5	6
(17)	(18)	(19)	(20)	(21)	(22)
Jumlah Permintaan		(23)			

II. Daftar Sertifikat Elektronik yang Diterbitkan
Bulan .....(24) Tahun .....(25)

No	Serial Number Sertifikat Elektronik	Nama Subjek	Masa Berlaku	Algoritma	Panjang Kunci
1	2	3	4	5	6
(26)	(27)	(28)	(29)	(30)	(31)
Jumlah Sertifikat Elektronik		(32)			

III. Daftar Permohonan Pembatalan Keabsahan Sertifikat Elektronik
Bulan .....(33) Tahun .....(34)

No	No. Surat Permohonan	Tanggal Permohonan	Serial Number Sertifikat	Nama Subjek	Keterangan
1	2	3	4	5	6
(35)	(36)	(37)	(38)	(39)	(40)
Jumlah Permintaan		(41)			

IV. Daftar Pembatalan Keabsahan Sertifikat Elektronik
Bulan .....(42) Tahun .....(43)

No	No. BA Pembatalan Keabsahan	Serial Number Sertifikat Elektronik	Nama Subjek	Tanggal Pembatalan	Keterangan
1	2	3	4	5	6
(44)	(45)	(46)	(47)	(48)	(49)
Jumlah Pembatalan		(50)			

V. Daftar Sertifikat Elektronik yang Diterbitkan Kembali
Bulan .....(51) Tahun .....(52)

No	Serial Number Sertifikat Elektronik	Nama Subjek	Masa Berlaku	Algoritma	Panjang Kunci
1	2	3	4	5	6
(53)	..... (54)	..... (55)	..... (56)	..... (57)	..... (58)
Jumlah Sertifikat Elektronik		..... (59)			

Petunjuk Pengisian Laporan Pengelolaan Kunci Kriptografi

1. Diisi dengan bulan pelaporan;
2. Diisi dengan tahun pelaporan;
3. Diisi dengan nomor laporan dengan mengacu pada penomoran internal Direktorat TIP;
4. Diisi dengan jumlah permintaan penerbitan pasangan kunci dan sertifikat elektronik pada bulan pelaporan untuk setiap kategori pemohon;
5. Diisi dengan jumlah penerbitan pasangan kunci dan sertifikat elektronik pada bulan pelaporan untuk setiap kategori pemohon;
6. Diisi dengan jumlah permohonan pembatalan keabsahan sertifikat elektronik yang diterima pada bulan pelaporan untuk setiap kategori pemohon;
7. Diisi dengan jumlah sertifikat elektronik yang dibatalkan keabsahannya pada bulan pelaporan untuk setiap kategori pemohon;
8. Diisi dengan jumlah penerbitan kembali pasangan kunci dan sertifikat elektronik yang diterbitkan kembali pada bulan pelaporan untuk setiap kategori pemohon;
9. Diisi dengan nama pejabat yang menyiapkan laporan;
10. Diisi dengan Nomor Induk Pegawai dari pejabat yang menyiapkan laporan;
11. Diisi dengan nama pejabat yang mengetahui laporan;
12. Diisi dengan Nomor Induk Pegawai dari pejabat yang mengetahui laporan;
13. Diisi dengan nama pejabat yang menyetujui laporan;
14. Diisi dengan Nomor Induk Pegawai dari pejabat yang manyetujui laporan;
15. Cukup jelas;
16. Cukup jelas;
17. Diisi dengan nomor urut;
18. Diisi dengan nomor surat permohonan penerbitan sertifikat elektronik;
19. Diisi dengan nama subjek yang mengajukan permohonan penerbitan sertifikat elektronik;
20. Diisi dengan organisasi dari subjek yang mengajukan permohonan penerbitan sertifikat elektronik;
21. Diisi dengan tanggal permohonan diajukan;
22. Diisi dengan keterangan yang dianggap perlu;
23. Diisi dengan jumlah permohonan penerbitan sertifikat elektronik yang diterima oleh Seksi Pengelolaan Intranet dan Internet;
24. Cukup jelas;
25. Cukup jelas;
26. Diisi dengan nomor urut;
27. Diisi dengan *serial number* dari sertifikat elektronik yang diterbitkan;
28. Diisi dengan nama subjek dari sertifikat elektronik yang diterbitkan;
29. Diisi dengan masa berlaku sertifikat elektronik;
30. Diisi dengan algoritma yang digunakan dalam sertifikat elektronik;
31. Diisi dengan panjang kunci yang digunakan;
32. Diisi dengan jumlah sertifikat elektronik yang diterbitkan pada bulan pelaporan;
33. Cukup Jelas;
34. Cukup Jelas;
35. Diisi dengan nomor urut;
36. Diisi dengan nomor surat permohonan pembatalan keabsahan sertifikat elektronik;
37. Diisi dengan tanggal pengajuan permohonan pembatalan sertifikat elektronik;
38. Diisi dengan serial number sertifikat elektronik yang diajukan pembatalan keabsahannya;
39. Diisi dengan nama subjek dari sertifikat elektronik yang diajukan untuk dibatalkan keabsahannya;
40. Diisi keterangan yang diperlukan terkait dengan permohonan pembatalan keabsahan sertifikat elektronik;
41. Diisi dengan jumlah permohonan pembatalan keabsahan sertifikat elektronik yang diajukan pada bulan pelaporan;
42. Cukup jelas;
43. Cukup jelas;
44. Diisi dengan nomor urut;
45. Diisi dengan nomor berita acara pembatalan keabsahan sertifikat elektronik;
46. Diisi dengan serial number dari sertifikat elektronik yang dibatalkan keabsahannya;
47. Diisi dengan nama subjek dari sertifikat elektronik yang dibatalkan keabsahannya;
48. Diisi dengan tanggal pembatalan keabsahan sertifikat elektronik;
49. Diisi dengan keterangan yang diperlukan terkait dengan pembatalan keabsahan sertifikat elektronik;
50. Diisi dengan jumlah sertifikat elektronik yang dibatalkan keabsahannya pada bulan pelaporan;
51. Cukup jelas;
52. Cukup jelas;
53. Diisi dengan nomor urut;
54. Diisi dengan serial number sertifikat elektronik yang diterbitkan kembali;
55. Diisi dengan nama subjek dari sertifikat elektronik;
56. Diisi dengan masa berlaku sertifikat elektronik yang diterbitkan;
57. Diisi dengan algoritma yang digunakan dalam sertifikat elektronik yang diterbitkan;
58. Diisi dengan panjang kunci yang digunakan dalam sertifikat elektronik yang diterbitkan;
59. Diisi dengan jumlah penerbitan kembali sertifikat elektronik pada bulan pelaporan.