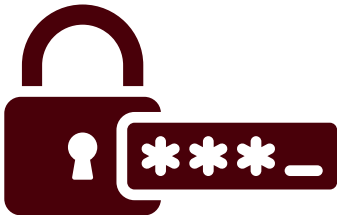
MENJAGA KEAMANAN PASSPHRASE
UNTUK TANDA TANGAN ELEKTRONIK TERSERTIFIKASI

Passphrase merupakan salah satu metode autentikasi yang harus dimasukkan saat seseorang ingin membubuhkan tanda tangan elektroniknya sehingga menjaga keamanan Passphrase menjadi hal yang penting agar tidak terjadi penyalahgunaan.



Risiko yang terjadi jika Passphrase bocor

Penyalahgunaan Identitas
Orang lain bisa menandatangani dokumen atas nama pemilik TTE.

Penyalahgunaan Wewenang
Berpotensi terjadinya penerbitan surat keputusan, perizinan, atau kebijakan yang melanggar hukum, yang dapat merugikan negara dan masyarakat.

Kerugian Finansial dan Hukum
Pemilik TTE akan menanggung beban hukum dan finansial dampak dari dokumen mengikat yang telah di TTE.

Rusaknya Reputasi dan Kepercayaan
Penyalahgunaan tanda tangan dapat merusak kepercayaan dan turunnya reputasi.

Langkah-langkah yang dilakukan jika Passphrase bocor

- Ubah/reset passphrase dengan passphrase baru yang Kuat
- Hubungi Penyelenggara Sertifikasi Elektronik (PSrE) jika tidak ada fitur reset mandiri
- Periksa dokumen yang ditandatangani atas nama anda, jika ada dokumen yang ditandatangani tanpa sepengetahuan anda, koordinasikan dengan pihak penerima dokumen serta laporkan ke PSrE atau penyedia TTE di instansi untuk dilakukan tindaklanjut.

Cara Agar Passphrase Aman

Buat Passphrase yang Kuat
Gunakan kombinasi huruf kapital, huruf kecil, angka, dan simbol. Hindari kata-kata yang mudah ditebak seperti tanggal lahir atau nama keluarga.

Jangan Bagikan Kepada Siapapun
Passphrase adalah rahasia pribadi yang hanya diketahui oleh pemiliknya, jangan pernah memberikannya kepada orang lain.

Waspada Serangan Phishing
Hati-hati dengan email, SMS, atau telepon yang meminta untuk memasukkan passphrase TTE.

Simpan dengan Aman
Jangan menyimpan di catatan ponsel yang tidak terlindungi. Manfaatkan aplikasi pengelola kata sandi (password manager) yang terpercaya jika sulit mengingat passphrase.

Ganti Secara Berkala
Sebagai langkah pencegahan tambahan, biasakan untuk mengganti passphrase Anda secara rutin, misalnya setiap 3-6 bulan sekali, terutama jika Anda merasa ada aktivitas yang mencurigakan.

Waspada Penggunaan Perangkat
Jangan gunakan perangkat umum atau wifi publik untuk mengakses atau menggunakan TTE. Pastikan perangkat pribadi terlindungi antivirus dan selalu diperbarui.

Manfaatkan MFA Jika Tersedia
Beberapa penyedia layanan TTE menawarkan fitur keamanan tambahan seperti MFA. Ini berarti, selain passphrase, Anda perlu memasukkan kode verifikasi yang dikirim ke ponsel atau email Anda. Aktifkan fitur ini untuk lapisan keamanan tambahan.

DISKOMINFOS PROVINSI BALI
PROGRAM LITERASI KESADARAN KEAMANAN SIBER
Ingin mendapatkan informasi terbaru dan konten literasi keamanan siber ?
Ayo berlangganan KABAR LENTERA (GRATIS !) di https://balikom.info/kabarlentera

SECURITY IS INCOMPLETE WITHOUT U #JagaRuangSiber
LENTERA SIBER
SAYA NETIZEN CERDAS

DISKOMINFOS.BALIPROV.GO.ID | diskominfosbali | diskominfos_bali | lenterasiber | balikom.info/link/lenterasiber
TLP: CLEAR

Balai Besar Sertifikasi Elektronik
Dokumen ini telah ditandatangani secara elektronik (TTE).
Scan/Klik QR Code untuk informasi TTE.
Upload file pada https://tte.komdigi.go.id/verifyPDF untuk cek keaslian file.
BANGGA BUATAN INDONESIA
BANGGA BERWISATA DI INDONESIA