PŘÍLOHA Č. 1 - DEFINICE POJMŮ A ZKRATEK

Pojem / Zkratka	Plný text	Vysvětlení
Asymetrická kryptografie	-----	Asymetrická kryptografie neboli kryptografie veřejných klíčů využívá dvojici klíčů (soukromý klíč a veřejný klíč) pro algoritmy šifrování a digitálního podepisování (např. algoritmy RSA, DSA atd.).
autentizace	-----	Proces ověření proklamované identity subjektu. Rozlišujeme autentizaci entity (osoby, programu) a autentizaci zprávy.
CA	Certifikační autorita	Souhrn technických a organizačně-administrativních prostředků, které umožňují vystupovat jako poskytovatel certifikačních služeb.
Certifikát	-----	Datová zpráva vydaná CA, která spojuje data pro ověřování podpisů (veřejný klíč) s identitou subjektu vlastnícího tato data.
CIA	Card Issuing Authority	Informační Systém Digitálního Tachografu.
CKG	Card Key Generator	Systém pro generování dávkové generování klíčů určených k uložení na kartu DT při personalizaci.
Company card	Karta podniku	Identifikace vlastníka vozu pro vyčtení relevantních dat.
Control card	Kontrolní karta	Identifikace kontrolního orgánu a vyčtení dat o průběhu jízdy.
CP	Card Personalization	Personalizace karet.
CPSUP		SW modul implementovaný na lince, který zajišťuje komunikaci personalizačního systému s čipovou kartou.
CSpSD	Centrum služeb pro silniční dopravu	Pracoviště MD pro příjem/výdej dat a expedici personalizovaných karet.
DB	Databáze	Databázový server pro uložení personalizačních dat.
DC_APP	Domain controller	Server, doménový server – server zajišťující personalizaci dávek karet DT.
Driver card	Karta řidiče	Pro autentizaci řidiče a spolujezdce a pro záznam jejich aktivit.
DT	Digital tachograph	Digitální tachograf - Záznamové zařízení určené pro montáž do silničních vozidel pro automatické nebo poloautomatické zobrazení, záznam a ukládání podrobností o pohybu takovýchto vozidel a o určitých pracovních dobách jejich řidičů.
EF.SOD	A RFC3369 CMS Signed Data Structure,	CMS struktura typu signed data, která obsahuje jednotlivé haše LDS datových skupin.
Evropská politika ERCA		Dokument „Digital Tachograf System European Root Policy" vydávaný Evropskou komisí.
HSM	Hardware Security Module	Hardwarový modul pro bezpečné uložení klíčů a provádění kryptografických operací.
IOKLIENT		Klientská stanice pro příjem a export dat – pro komunikaci s KISDT, načítání vstupních dávek pro výrobu, distribuce výstupních dávek, expedice karet, tisk nosičů a PIN obálek.
ISDT		Informační Systém Digitálního Tachografu.
JPK		Klientská stanice pro řízení personalizace.
Karta DT		Čipová karta, určená k užití s Digitálním tachografem. Karta DT umožňuje v záznamovém zařízení identifikaci totožnosti (nebo skupiny totožností) držitele karty a umožňuje převod údajů a jejich ukládání. Dle právní úpravy účinné ke dni uzavření Smlouvy karta může být čtyř typů: (i) karta řidiče, (ii) karta podniku (vozidla), (iii) karta dílny (servisu) a (iv) karta kontrolní. V případě legislativních změn zavádějících nový typ či typy karet se Kartou DT dle Smlouvy rozumí i takovýto nový typ či typy čipové karty.
KISDT	klient ISDT	Klientská stanice KISDT je určena k obousměrné komunikaci mezi systémem sběru a přípravy dat (ISDT) a personalizačním systémem.
Kořenový certifikát	-----	Certifikát, vystavený CA pro svůj veřejný klíč, podepsaný odpovídajícím soukromým klíčem ("self-signed" certifikát).
MSA	Member State Authority = CZA	Státní orgán zodpovědný za systém DT (Ministerstvo dopravy).

Pojem / Zkratka	Plný text	Vysvětlení
MSCA	Member State Certification Authority = CZCA	CA pro dávkové generování certifikátů určených k uložení na Kartu DT při personalizaci.
Národní certifikační politika/NCAP	National CA Policy	Resortní politika certifikačních orgánů pro systém Digitální tachograf v České republice.
neslučitelnost rolí	-----	Nepřípustná kombinace dvou rolí, vykonávaná jednou osobou.
netHSM	Síťový HSM	Kryptografické moduly – zařízení pro bezpečné uložení citlivého klíčového materiálu.
ORP		Obec s rozšířenou působností.
Osobní údaj	-----	Jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.
PG	PIN management	Systém pro generování PINů pro karty dílny DT.
PSDT	Personalizační SW digitálního tachografu	Personalizační software pro personalizaci Karet DT.
PIN	Personal identification number	Osobní identifikační číslo.
Projekt DT		Projekt Digitálního tachografu České republiky, zahrnující poskytování služeb výroby a personalizace Karet DT a služby provozu a podpory ISDT.
Projektová kancelář STC		Organizační jednotka objednatele; může zahrnovat i externí subjekty podílející se na Projektu DT.
Specimen	-----	Vzor Karty DT.
STC	STÁTNÍ TISKÁRNA CENIN, státní podnik	Poskytovatel služby DT pro Ministerstvo dopravy
symetrická kryptografie	-----	Používá k šifrování i dešifrování jediný klíč.
Token		Kryptograficky zabezpečená datová struktura obsahující identifikátory aplikace a jeho otisk určená pro vzdálenou správu aplikací realizovaných přes dodatečné bezpečnostní domény (SSD).
VYSTKONT	Výstupní kontrola	Pracoviště pro kontrolu správnosti personalizovaných Karet DT.
Workshop card	Karta dílny	Identifikace servisního technika a uložení symetrických klíčů pro zavedení do snímačů a jejich kalibraci.
Zadavatel MD		Česká republika - Ministerstvo dopravy, které je zadavatelem veřejné zakázky a se kterým má objednatel uzavřenou smlouvu o poskytování služeb „Výroba a personalizace karet digitálního tachografu České republiky“.
Zneplatněný certifikát	-----	Certifikát, u nějž byla ukončena platnost bez možnosti obnovy této platnosti a který je uveden v seznamu CRL.
Zpracovatel	-----	Ve smyslu zákona na ochranu osobních údajů (zákon č. 101/2000 Sb.) je to každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.