SOUDNÍ INŽENÝRSTVÍ

Ročník 32 • 4/2021
Doprava • Transportation

www.soudniinzenyrstvi.cz

Použití kryptografie v soustavě tachografu

Application of Cryptography in a Tachograph System

Ondřej Koutník[a*], Štěpánka Doleželová[b]

[a]*Vysoké učení technické v Brně, Ústav soudního inženýrství, Brno*
[b]*Centrum dopravního výzkumu, v.v.i., Brno*

Abstrakt

Článek se zabývá kryptografií v kontextu tachografů a silniční nákladní dopravy. Podstatou tachografu je zaznamenávat činnosti řidičů. Neoprávněným zásahem do této vozidlové soustavy lze dosáhnout výhod pro řidiče nebo dopravce. Pro zajištění vybraných parametrů týkajících se bezpečnosti se využívá kryptografických mechanismů, které musí poskytovat určitou míru teoretické neprolomitelnosti. S ohledem na růst výpočetního výkonu je potřeba použité algoritmy a délky klíčů pravidelně aktualizovat, což ilustrují i změny algoritmů během vývoje jednotlivých verzí a generací tachografu.

Klíčová slova: bezpečnost, kryptografie, nákladní doprava, tachograf, šifrování.

Abstract

The article is focused on cryptography in the context of tachographs and road freight transport. The main task of tachograph is to record activities of drivers. Unauthorized tampering with this on-board system can provide benefits for the drivers or carriers. Selected security parameters are ensured by using certain cryptographic mechanisms, which must provide a specific level of theoretical breaking resistance. As computing power permanently increases, it is necessary to regularly update the algorithms and encryption key lengths used, which is illustrated by the changes in algorithms during development of different generations and versions of tachographs.

Keywords: cryptography, encryption, freight transport, tachograph, security.

POUŽITÉ ZKRATKY

AES	Advanced Encryption Standard standard pokročilého *šifrování* – symetrick*á šifra.*
DES	Data (Digital) Encryption Standard – symetrická *šifra.*
ECC	Elliptic-Curve Cryptography – Kryptografie eliptických křivek – asym. *šifr*a.
FIPS	Federal Information Processing Standard.
GNSS	Global Navigation Satellite System – Globální družicový polohový systém.
KITAS	Obchodní název pro snímače společnosti VDO Continental.
MS	Motion sensor – snímač pohybu.
MAC	Message authentication code – autentizační kódy zpráv.
RSA	Asymetrická *šifra* (název tvoří inciciály autorů).
TC	Tachograph card – karta tachografu.
VU	Vehicle unit – vozidlová jednotka – záznamové zařízení.

1. ÚVOD

Komunikace je proces, při kterém dochází k předávání informací od odesilatele k příjemci nebo příjemcům. Tyto informace mohou představovat vstup do dalších rozhodovacích procesů, a proto je již historicky patrná snaha zajistit určité parametry přenášených informací. Jedná se o zajištění důvěrnosti, autentičnosti, neodvolatelnosti a integrity dat. Pro tyto účely lze využít algoritmy šifrování. Věda, která se šifrováním zabývá se nazývá kryptografie.

S rozvojem elektroniky ve vozidlech, která kromě komfortu osádky zajišťuje také bezpečnostní a provozní parametry provozu, vznikla potřeba zajistit vybrané zmíněné parametry některých přenášených informací (dat) tak, aby se zabránilo možnému ovlivnění klíčových funkcí nebo zjištění utajovaných informací třetí osobou.

Tento článek představí vybrané šifrovací mechanismy u soustavy inteligentního tachografu, který dle příslušných právních předpisů zajišťuje záznam činností řidiče automobilu převyšujícího celkovou

Dodáno do redakce: 1. 9. 2021
Recenzní řízení: od 20. 09. 2021 do 4. 10.2021

DOI: http://dx.doi.org/10.13164/SI.2021.4.3

**Korespondenční adresa: ondrej.koutnik@vutbr.cz*

hmotnost 3 500 kg a slouží pro jejich kontrolu. Vychází se tak z faktu, že únava z řízení nebo jiných činností řidiče (nakládka, údržba vozidla…) má výrazný vliv na bezpečnost řízení daného vozidla, potažmo na bezpečnost silničního provozu. Je zde tedy patrné vyšší riziko negativní události a díky vyšší hmotnosti vozidla i vyšší pravděpodobnost závažných škod nebo újmě na zdraví účastníků provozu.

2. ZÁKLADNÍ POPIS TACHOGRAFU

Soustava tachografu je složena ze záznamového zařízení instalovaného v kabině vozidla, ze snímače pohybu, instalovaného nejčastěji v otvoru převodové skříně vozidla a kabeláže, která spojuje snímač a záznamové zařízení. Pro ukládání dat je určena interní paměť záznamového zařízení a paměťové karty tachografu, které jsou vybaveny čipem. Karta tachografu slouží pro identifikaci uživatele, kterými jsou řidiči, pracovníci dílny, dopravci a kontrolní pracovníci.

O podíl na trhu záznamových zařízení se většinově dělí společnosti VDO Continental Automotive GmbH a Stoneridge AB. Dále jsou na trhu také další společnosti, které mají menší podíl, např. Intellic GmbH nebo ASELAN. U snímačů pohybu převažuje výrobce VDO Continental se svou řadou snímačů KITAS. Menší podíl zastupuje firma Lešikar.

Soustava tachografu má vybrané parametry a funkce definované na úrovni Evropské unie, a to následujícími předpisy:

- **Analogový tachograf**: Příloha I Nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě, o zrušení nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě a o změně nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy.
- **Digitální tachograf**: Příloha IB Nařízení Rady (EHS) č. 3821/85 ze dne 20. prosince 1985 o záznamovém zařízení v silniční dopravě, ve znění všech změn.
- **Inteligentní tachograf 1. a 2. verze**: Příloha IC Prováděcí nařízení Komise (EU) 2016/799 ze dne 18. března 2016, kterým se provádí nařízení Evropského parlamentu a Rady (EU) č. 165/2014, kterým se stanoví požadavky na konstrukci, zkoušení, montáž, provoz a opravy tachografů a jejich součástí.

Nejstarší předpisy specifikovaný tachograf je analogový a podstatou jsou mechanické nebo elektronické vazby bez využití šifrování. Záznam byl zaznamenáván zapisovací jehlou na papírový kotouč s vhodnou úpravou horní zapisovací vrstvy. V současné době jsou ve vozidlech zastoupeny v řádu jednotek procent. Od května 2006 byly zavedeny k instalaci do vozidel digitální tachografy využívající k zápisu signály generované snímačem pohybu a elektronické paměti. Tato generace prošla několika úpravami s ohledem na funkce a bezpečnostní prvky. Od 15.června 2019 byla zavedena nová generace tachografů – tzv. inteligentní tachografy. Tyto tachografy využívají obdobně elektrický signál a paměti a zahrnují také přijímač GNSS signálu. Bezpečnostní mechanismy byly znovu vylepšeny. Postupně bude dle nařízení (EU) 165/2014 docházet k nahrazení zmíněných verzí tachografů za druhou verzi inteligentních tachografů, které mají další funkce dle vývoje souvisejících předpisů. Do poprvé registrovaných vozidel na území EU budou tyto tachografy instalovány od srpna 2023.

3. KRYPTOGRAFIE A BEZPEČNOST

Kryptografie je věda zabývající se matematickými algoritmy, které slouží pro změnu prvků v bitovém řetězci zprávy tak, aby měla pro neoprávněnou osobu minimální nebo ideálně žádnou informační hodnotu. Zajišťuje zejména autenticitu, důvěrnost, nepopiratelnost a integritu posílaných zpráv. Důvěrností se rozumí parametr, kdy je obsah zprávy znám pouze odesílateli a příjemci. Pokud je zpráva autentická, příjemce má jistotu, že původce je skutečným odesílatelem v avizovaném čase a místě vytvoření. Neodvolatelnost, resp. nepopíratelnost znamená nemožnost popřít dříve komunikované informace. Integrita pak zaručuje úplnost a originalitu, resp. nezměněný obsah zprávy.

Obecně lze dle [1] rozlišovat kryptografické algoritmy a protokoly dle jejich principů a určení na:

- symetrické algoritmy,
- asymetrické algoritmy,
- protokoly (algoritmy) pro zajištění autenticity dat,
- algoritmy pro zajištění integrity dat.

U symetrických systémů vlastní každá z komunikujících stran shodný klíč. Obecně tyto systémy dosahují vyšší rychlosti šifrování, avšak v praxi je složitější bezpečný přenos klíčů.

U asymetrických systémů se obecně vychází z obtížně řešitelných matematických operací (např. problém faktorizace velkého čísla, diskrétní logaritmus nad eliptickou křivkou …) a využívají se jednosměrné matematické funkce, tzn. že bez znalosti soukromého klíče lze jen velice obtížně zjistit původní zprávu. S ohledem na délku klíče musí být kryptografické systémy za dobu rezistence prakticky neprolomitelné. Doba rezistence se liší v závislosti na konkrétní aplikaci v daném zařízení, resp. na použitém algoritmu a délce klíče.

Zajištění úrovně bezpečnosti soustavy tachografu se řeší zejména certifikací podle standardu Common Criteria for Information Technology Security Evaluation a požadavky týkající se bezpečnosti jsou stanoveny také v příslušných předpisech Evropské Unie, které se vzájemně s uvedeným standardem na sebe odkazují. Tyto předpisy využívají i informací a postupů uvedených v dalších „podpůrných" standardech definujících vybrané postupy (např. ISO 16844-3, ISO/IEC 7816-4, ISO/IEC 9796-2, FIPS PUB 197). Využívá se také mechanismů osvědčení (bezpečnost, funkčnost, interoperabilita), které jsou podkladem pro vydání osvědčení o schválení typu jednotky ve vozidle, snímače pohybu a karty tachografu.

4. BEZPEČNOSTNÍ PARAMETRY

Common Criteria for Information Technology Security Evaluation (zkráceně jen Common Criteria nebo CC) je mezinárodní standard označovaný také jako (ISO/IEC 15408), který slouží pro hodnocení produktů v oblasti informačních technologií. Systém je založen na žadateli, který má zájem o certifikaci svého produktu, certifikované laboratoři, která provádí testování, a autoritě, která na celý proces dohlíží.

Jsou definovány dokumenty standardu [2]:

- Protection Profile (v odborné terminologii označován zkratkou PP) – základní sada obecně použitelných bezpečnostních parametrů, které by měl daný výrobek splňovat a jejich odůvodnění.
- Security Target (v odborné terminologii označován zkratkou jako ST) – upřesnění parametrů v PP na konkrétní objekt hodnocení – Target of Evaluation (TOE), viz dále.

Oba dokumenty v úvodu obecně definují prostředí soustavy tachografu a související bezpečnostní problém, resp. zájmy, které mají být ochráněny (integrita, důvěrnost dat apod.). Poté jsou stručně uvedeny hrozby, předpoklady a bezpečnostní politiky tykající se objektu hodnocení. Dále jsou stanoveny bezpečnostní cíle objektu a rozšiřujících komponentů. Poté jsou specifikovány bezpečnostní funkční požadavky a zdůvodnění zvolených parametrů. V jednotlivých částech dokumentů se užívá hierarchické dělení prvků na třídy, rodiny, komponenty a elementy.

Obecně jsou užívány a definovány pojmy:

- Target Of Evaluation (TOE) – jedná se o konkrétní produkt – objekt hodnocení.
- Evaluation Assurance Level (EAL) – definuje obtížnost zkoušky, přičemž EAL1 je nejnižší úroveň a EAL7 je nejvyšší úroveň. Obvykle se pro komerční produkty využívá úroveň nejvýše EAL 4 [3].
- Obecná rizika („*threats*“), které jsou označována například jako T.Output_Data, nebo T.Card_Data_Exchange.
- Premise provozních podmínek („*assumptions*“), za kterých jsou zajištěny bezpečnostní funkce. Označují se např. A.Approv_Workshops.
- Bezpečnostní politiky („*organisational policies*“) – odkazuje na závazné předpisy – např. P.Crypto odkazuje na prováděcí nařízení EU.
- Bezpečnostní záměry („*objectives*“), které v návaznosti na v úvodu definovaný problém obecně popisují kroky nebo podmínky, které musí být dodrženy pro zachování bezpečnosti. Jedná se např. o O.Output.
- Rozšířené komponenty – „složky záruky“ („*assurance components*“), V případě tachografu např. ATE_DPT.2 nebo AVA_VAN.5, které na vyšší úrovni než EAL4 stanovují požadavky na testování funkcí nebo testování resistence proti útokům.

Druhy použitých funkcí šifrování jsou specifikovány v přepisu EU [4] a jsou zvoleny v souladu s technologickým pokrokem a s ohledem na konkrétní využití, a to se zohledněním algoritmu a délky řetězce kryptogramu. Využívá se také hešovacích a pečetících funkcí a certifikátů. Digitální certifikát se připojuje k určitým informacím (např. vlastnictví veřejného klíče, platnost certifikátu nebo čas vzniku zprávy) a je vydaný důvěryhodnou autoritou. Certifikáty se využívají jak záznamovém zařízení, tak i v kartách do tachografu.

5. ASPEKTY BEZPEČNOSTI

Při vývoji soustavy tachografu podobně jako u jiných „embedded“ systémů dochází ke kompromisu mezi cenou a úrovní bezpečnosti. Schopnost uplatnit výrobek na trhu závisí na mnoha faktorech, přičemž nezanedbatelnou roli hraje faktor prodejní ceny. Cena tak určuje parametry použitého hardware a software (např. rychlost a s tím související zvolený algoritmus šifrování a délku klíče). Přesto, že je manipulace s tachografem považována evropským předpisem za velmi závažné porušení, nachází se na druhé straně obchodní, výrobní, ekologické a další aspekty, které se odráží ve výsledné nastavené úrovni zabezpečení. Obecně platí, že čím je vyšší složitost soustavy (počet prvků, varianty provozu atp.), tím složitější a náročnější je i zajištění bezpečnostních parametrů.

Příloha IC prováděcího nařízení 799/2016 i Common Criteria specifikuje Protection Profile (v české verzi nařízení „profil ochrany“) pro jednotlivé prvky soustavy tachografu [4]:

- profil ochrany celku ve vozidle,
- profil ochrany karty tachografu,
- profil ochrany snímače pohybu,
- profil ochrany vnějšího zařízení GNSS.

Útoky na soustavu tachografu jsou známy z odborných seminářů a dostupné judikatury (např. 6 As 101/2019–28) výhradně ze strany řidiče nebo dopravce, protože jedině ti mají objektivně z podvodného jednání benefity. Navíc mají časově neomezený a volný přístup k prvkům soustavy. Prostředí pro uskutečnění podvodu je nejčastěji fyzický prostor vozidla, avšak technické možnosti nevylučují ani dálkový zásah např. prostřednictvím komfortní elektroniky nebo přidaného rozhraní pro bezdrátovou komunikaci (mobilní datové komunikace…). Způsob provedení závisí na více faktorech – zejména na ceně, potřebných znalostech, náročnosti na provedení a na možnosti detekce. Aktuálně jsou dle kontrolních složek známy i případy manipulace se softwarem soustavy tachografu, kde lze očekávat i ovlivnění funkcí šifrování. Pro ilustraci rozsahu problému lze využít i zprávu Spolkového ministerstva dopravy a digitální infrastruktury k prevenci nehod, která v oblasti manipulací s tachografem uvádí za rok 2019 míru závadovosti ve výši 19 procent ze všech kontrolovaných vozidel. Znamená to tedy, že téměř každé páté vozidlo, které prošlo kontrolou tachografu mělo zjištěno závadový stav v podobě zařízení zasahujícího do činnosti tachografu [5]. Útoky na soustavu tachografu lze rozlišovat podle motivace k manipulaci:

Motivační impuls **ze strany dopravce**:

- snaha o vyšší zisk v podobě vyššího dopravního výkonu vozidla,
- snaha o konkurenční výhodu oproti jiným dopravcům (kompenzace k nedostatku řidičů, pokrytí výkyvů poptávky apod.).

Motivační impuls **ze strany řidiče**:

- snaha o kompenzaci organizačních a provozních nedostatků – např. snížení doby prostojů, dřívější návrat domů,
- motivace vyšší mzdou.

Z uvedeného je patrné, že dochází k ovlivnění zápisu činnosti „jízda“ a „přestávka/odpočinek“ k tomu, aby byly zdánlivě dodrženy požadavky na dobu řízení stanovené nařízením (ES) 561/2006. Ve skutečnosti se během pohybu vozidla zaznamenává činnost pro „přestávku/odpočinek“. Útok se tedy klasifikuje jako aktivní útok na zařízení, s cílem změny komunikačního toku. Metody manipulací s tachografem v čase prochází vývojem, který

v současné době provádí jednotlivci nebo týmy s vysokou odbornou úrovní. Vývoj tak reaguje na schopnosti a znalosti kontrolních orgánů a v okamžiku, kdy dojde k odhalení, tak na základě získaných informací vývojáři pravděpodobně upravují technické řešení vedoucí k zamezení odhalení. Aspekty bezpečnosti soustavy tachografu tedy spočívají v:

- zabránění neoprávněného přístupu a změně dat v paměti tachografu nebo uložených v paměti karty tachografu,
- zabránění neoprávněných vlivů na komunikaci mezi jednotkou a snímačem pohybu nebo mezi jednotkou a kartou tachografu,
- zabránění neoprávněných vlivů na komunikaci mezi jednotkou a GNSS, případně jednotkou a DSRC zařízením – zajištění integrity a autenticity dat.

6. POUŽÍVANÉ KRYPTOSYSTÉMY

Soustava tachografu využívá pro zajištění definovaných bezpečnostních parametrů komunikace šifrovací algoritmy, a to jak symetrické, tak asymetrické.

U symetrických algoritmů šifrování se používá pouze jeden klíč, který je tajný a držiteli klíče jsou obě komunikující strany. Jak je zmíněno výše, aby byly zachovány požadované parametry zařízení, prochází tyto elektronické záznamové soustavy vývojem. Ten zahrnuje jak vývoj funkcí odrážející potřeby dopravního sektoru, tak i vývoj odrážející vývoj v kryptografii a výpočetní technice.

U tachografů digitálních se tak využívá blokový symetrický šifrovací algoritmus Triple DES (TDES nebo 3DES), který je založen na algoritmu DES a při šifrování dochází k využití Feistelovy šifry. To spočívá v rozdělení bloku zprávy na levou a pravou část, přičemž pravá část současně s klíčem vstupuje do konverzní funkce a výsledek je poté zpracován logickou operací „XOR" k levé části bloku zprávy. Obě výsledné části jsou prohozeny tak, aby například levá část vstupního bloku byla pravou částí výstupního bloku. V tachografech se využívá dělení klíčů, kdy část klíče je vložena do karet dílny a část je v záznamovém zařízení. Výsledný hlavní klíč je výsledkem logické operace XOR těchto dvou klíčů. Hlavní klíč se pak užívá k autentizaci mezi jednotkou a snímačem pohybu. Dále se odvozuje pomocí TDES identifikační klíč K_{id}, a volí párovací klíč K_p a klíč relace K_s.

U inteligentních tachografů jsou klíče K_m, K_{wc} a K_p, K_{id} a K_s vytvořeny na základě symetrického blokového šifrovacího algoritmu AES, jehož podstatou je střídání matematických operací permutace a substituce. Výhodou také je, že dokáže pracovat s delším řetězcem bloku a zpracování řetězce tímto algoritmem je rychlejší. Zároveň je možnost využívat i klíče délky 256 bitů oproti maximu 168 bitů u TDES. Princip TDES je zachován pouze u dočasného klíče relace užívaného pro komunikaci mezi jednotkou a kartou tachografu.

U asymetrických algoritmů šifrování jsou klíče dva, a to veřejný a soukromý klíč. Soukromý klíč je tajný, veřejný klíč je volně přístupný. Mechanismus přidělení klíčů je založen na PKI – infrastruktuře veřejných klíčů, která definuje úrovně [4]:

- evropská úroveň,
- úroveň členského státu,
- úroveň zařízení.

Z asymetrických algoritmů se v tachografech využívá algoritmus RSA (digitální tachografy), který je založen na principu faktorizace (rozklad čísla na součin dvou prvočísel) dvou dostatečně velkých prvočísel, přičemž za dostatečně velké prvočíslo se považuje číslo o velikosti alespoň 2048 bitů. V digitálních tachografech dominuje asymetrický algoritmus RSA o parametrech modulu n = 1 024 bitů, veřejného exponentu e = 64 bitů a soukromého exponentu d = 1 024 bitů [4].

Za nástupce RSA systému, který se uplatňuje v inteligentních tachografech, se označuje šifrování na bázi eliptických křivek (ECC), které je rychlejší a při zachování stejné úrovně bezpečnosti si vystačí s kratším klíčem. Na bezpečnost má vliv tvar použité eliptické křivky. Přičemž podstata spočívá v problému výpočtu parametru diskrétní logaritmu nad eliptickou křivkou při neznalosti všech vstupních údajů. Výpočet vychází ze vztahu: $z = x^y \bmod n \Leftrightarrow \log_x z = y \bmod n$, kde je patrné že výpočet hodnoty z je při znalosti proměnných x, y, n poměrně rychlý a jednoduchý. Pokud však proměnnou y ponecháme jako soukromou hodnotu, bude výpočet z bez této znalosti proměnné y velice složitým.

U doménových parametrů kryptosystému založeného na eliptických křivkách si výrobci tachografů nemohou zvolit doménové parametry samostatně, ale musí využít specifikované domény v příloze IC nařízení 2016/799. Tyto parametry jsou uvedeny v následující tabulce (tab. 1).

Pro zajištění jistoty původu veřejného klíče se užívá digitálních certifikátů veřejného klíče. K jeho ověření a následnému podepisování zpráv se využívá i hešovacích nebo pečetících

Tab. 1 Algoritmy pro ECC šifrování.
Tab. 1 Algorithms for ECC cyphering.

Název	délka klíče v bitech
NIST P-256	256
BrainpoolP256r1	256
NIST P-384	384
BrainpoolP384r1	384
BrainpoolP512r1	512
NIST P-521	521

Zdroj: [4]

Tab. 2 Šifrovací sady.
Tab. 2 Cypher suites.

Sada	ECC délka klíče v bitech	AES délka klíče v bitech	Hešovací algoritmus	Délka MAC
CS #1	256	128	SHA-256	8
CS #2	384	192	SHA-384	12
CS #3	512/521	256	SHA-512	16

Zdroj: [4]

Tab. 3 Účel kryptografie v IT tachografu.
Tab. 3 Purpose of cryptography in IT tachograph.

AES – symetrický blokový algoritmus	
Párování VU[1] a MS[2]	
Vzájemná autentizace mezi VU a MS	
Zajištění důvěrnosti a integrity přenášených dat mezi VU a MS	
Zajištění důvěrnosti a integrity přenášených dat mezi VU a TC[3]	
Zajištění důvěrnosti přenášených dat mezi VU a TC (tam, kde lze)	
Zajištění autenticity a integrity přenášených dat mezi VU a externím GNSS[4]	
ECC – šifrování na bázi eliptických křivek	
Vytvoření digitálního podpisu (ECDSA)	
Verifikace digitálního podpisu	
Ustavení kryptografických klíčů	
Vzájemná autentizace mezi VU a TC	
Zajištění párování VU a externího GNSS	
Zajištění autentizace mezi VU a externím GNSS	
Zajištění autentizace, integrity a nepopíratelnosti u stahovaných dat	
[1]VU = jednotka ve vozidle	[3] TC = Karta tachografu
[2] MS = senzor pohybu	[4] GNSS = globální navigační satelitní systém

Zdroj: autor s využitím [4, 7]

funkcí, které představují zkrácený důvěryhodný „otisk“ zprávy. U digitálních tachografů se využívá algoritmus SHA-1, který byl v inteligentních tachografech povýšen na SHA 256, 384 nebo 512 (dle zvolené šifrovací sady), viz tab. 2. U inteligentních tachografů se kromě hešovacích funkcí využívají i pečetící funkce MAC (Message authentication code), které se z anglického překladu nazývají autentizační funkce zpráv. Oproti hešovacím funkcím, které zajišťují integritu zprávy, MAC zajišťují i autenticitu, protože do pečetící funkce vstupuje i soukromý (tajný) klíč.

Ze společných vlastností hešovacích algoritmů lze jmenovat jednosměrnost hešovací funkce, nemožnost nalézt z množiny hešů jinou původní zprávu, a nemožnost nalézt dvě zprávy se stejným hešem.

Pro inteligentní tachografy tak byly stanoveny šifrovací sady, které určují povolené kombinace algoritmů a délky klíčů, viz tab. 2.

S vývojem výpočetního výkonu počítačů, musí pro zajištění bezpečnosti korespondovat i procesy udržování neprolomitelnosti u použitých algoritmů, a to s ohledem na vývoj výkonu klasických digitálních počítačů, který se přibližně řídí Moorovým zákonem. Ten říká, že výkon se každých osmnáct měsíců zdvojnásobí dvakrát při zachování stejných nákladů [6]. Zohledněn musí být i vstup výkonných kvantových počítačů do komerční sféry. Na sílu, resp. odolnost šifry má vliv zejména použitý algoritmus (resp. záleží, na kterém matematickém problému je založený) a délky klíčů. Pro přirozenou obnovu technických prostředků a umožnění udržování vývoje se využívá omezené délky platnosti certifikátů. Následující tabulka (tab. 3) tak znázorňuje zobecněné použití kryptografie v soustavě inteligentních tachografů.

Dne 30. 7. 2021 vyšla v Úředním věstníku Evropské unie (pod označením 2021/1228) změna prováděcího nařízení (EU) 2016/799, která však nemění používané kryptografické algoritmy a přidává tachografu vybrané funkce v souladu s předpisy.

Kryptografie tvoří v soustavě tachografu bezpečnostní prvek zabraňující podvrhnutí komunikace a záměně prvků za neznámé zařízení třetí strany. Jedině znalost správných klíčů a komunikačního protokolu umožňuje zašifrovat zprávy do kryptogramu, který bude srozumitelný příjímací entitě a zajištěný proti ovlivnění třetí stranou. Omezená časová platnost jednotlivých certifikátů zajišťuje, aby nebyly kryptografické mechanismy prolomeny před dobou své rezistence.

V současné době jsou certifikáty omezeny platností v různých délkách v řádu let v závislosti na typu certifikátu. Pro karty tachografu (hlavní i podpisový klíč) se tak jedná o jeden, dva nebo pět let v závislosti na kategorii uživatele, resp. typu karty. Pro tachografy je pak platnost certifikátů stanovena na 15 let a 3 měsíce. Kořenový certifikát Evropské certifikační autority je pak platný 34 let a certifikát pro komunikaci s externím GNSS má platnost 15 let [4].

7. ZÁVĚR

S vývojem tachografů je patrný i vývoj na poli kryptografie v těchto soustavách. Pro zajištění bezpečnosti soustavy tachografu je nezbytná komplexní analýza nejen vnitřního, ale i vnějšího prostředí. Jak již bylo zmíněno, nástup 2. verze inteligentního tachografu se očekává v roce 2023 a zároveň se počítá od června 2026 s povinným rozšířením tachografů i do vozidel v rozmezí hmotnosti 2500–3500 kg v mezinárodní přepravě. Tím, že se výrazným počtem rozšíří uživatelská základna tachografů, lze oprávněně očekávat zvýšení intenzity úsilí věnované vývoji metod neoprávněných manipulací, a to zejména s ohledem na fakt, že uplatnění relevantních předpisů, a tedy i tachografu, k omezení doby řízení řidiče může citelně ovlivnit ziskovost předmětných vozidel.

Pro kvalitní a účinné kontroly je tedy naprosto nezbytné reagovat na zvýšení počtu vozidel s tachografem navýšením kapacit kontrolních míst tak, aby došlo k zachování míry prokontrolovanosti (aktuálně nejméně 3 % pracovních dnů řidičů vozidel, na něž se

vztahují přímo použitelné předpisy Evropské unie [8]) vozidel a udržel se tak i žádoucí efekt odrazení od podvodného jednání. Toho se snaží kontrolní složky dosáhnout například pořizováním zařízení pro včasnou dálkovou komunikaci s tachografem tak, jak to stanovují také předpisy Evropské unie, pořizováním zařízení na odhalování manipulací s tachografem, případně lze zmínit využívání poloautomatického softwaru pro vyhodnocování zaznamenaných dat tachografem.

Znalci specializující se na tachografy tak mohou do budoucna čelit požadavkům na posudky, ve kterých jim budou předloženy prvky soustavy tachografu, v níž útočník kompromitoval soukromé klíče dříve než vypršela jejich doba rezistence, případně prolomil kryptografickou ochranu. To umožňuje útočníkům neoprávněně upravit funkční algoritmy prvků nebo uložená data touto soustavou s omezenou škálou manipulačních indicií. Dne 30. 7. 2021 vyšla v Úředním věstníku Evropské unie změna prováděcího nařízení 2016/799 s označením 2021/1228, které specifikuje požadavky na inteligentní tachografy. Nově je zde také funkce pro aktualizaci softwaru záznamového zařízení, což sice snižuje náklady na generační obměnu, ale na druhé straně může představovat rozhraní pro uskutečnění neoprávněného zásahu.

V současné době se vypracovává studie proveditelnosti k návrhu mobilní aplikace TachograpApp, která by mohla v budoucnu nahradit, případně doplňovat současnou soustavu tachografu ve vozidle. Potřebné vhodné technologie a nástroje, včetně sledování polohy a záznamu činnosti řidiče, jsou již vyvinuté. Zbývá tak analyzovat zejména otázky ekonomické a bezpečnostní. I v případě mobilní aplikace budou bezpečnostní parametry klíčové. Mimo další výhody lze také zmínit možnosti autentizace s využitím dokazování biometrickými parametry. Ať už je v budoucnu technické řešení záznamu zvoleno mobilní aplikací nebo současným způsobem, kryptografie bude v obou případech hrát významnou roli.

Tento článek byl vytvořen za finanční podpory Ministerstva dopravy v rámci programu dlouhodobého koncepčního rozvoje výzkumných organizací.

8. LITERATURA

[1] STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. Seventh edition, Global edition. Essex, England: Pearson Education Limited, 2017. ISBN 10 1-292-15858-1.

[2] STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. Fourth Edition. Upper Saddle River, New Jersey, United States of America: Pearson Prentice Hall, 2006. ISBN 10 0-13-187316-4.

[3] ANDERSON, R. *Security engineering: a guide to building dependable distributed systems*. 2nd ed. Indianapolis: Wiley, 2008. ISBN 978-0470068526.

[4] Prováděcí nařízení komise (EU) 2016/799, kterým se provádí nařízení Evropského parlamentu a Rady (EU) č. 165/2014, kterým se stanoví požadavky na konstrukci, zkoušení, montáž, provoz a opravy tachografů a jejich součástí. Konsolidované znění. In: Úřední věstník Evropské unie. L 139, 26.5.2016, s. 1. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:02016R0799-20200226

[5] Deutscher Bundestag – Unterrichtung durch die Bundesregierung: Bericht der Bundesregierung über Maßnahmen auf dem Gebiet derUnfallverhütung im Straßenverkehr 2018 und 2019 (Unfallverhütungsbericht Straßenverkehr 2018/2019) [online]. 19. Wahlperiode. Berlin, 2021 [cit. 2021-8-30]. ISSN 0722-8333. Dostupné z: https://www.bmvi.de/SharedDocs/DE/Artikel/K/unfallverhuetungsbericht-2018-2019.htm

[6] PAAR, CH., PELZL, J. *Understanding cryptography: a textbook for students and practitioners*. Heidelberg: Springer, 2010. ISBN 978-3-642-04100-6.

[7] Common Criteria Protection Profile: Digital Tachograph Vehicle Unit [online]. Ispra (Italy, VA): DG JRC Directorate E Space, Security and Migration, 2021 [cit. 2021-8-30]. Dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0094b_pdf.html

[8] Vyhláška č. 522/2006 Sb.: Vyhláška o státním odborném dozoru a kontrolách v silniční dopravě, ve znění 30.08.2021. In: . Praha, 2006, 522/2006. Dostupné také z: https://www.zakonyprolidi.cz/cs/2006-522/zneni-20201001

Správná citace:
KOUTNÍK, O.,DOLEŽELOVÁ, Š. Použití kryptografie v soustavě tachografu. *Soudní inženýrství*, 2021, 32(4), 3–8.
DOI: http://dx.doi.org/10.13164/SI.2021.4.3. ISSN 1211-443X.