

УДК 658.1.004

МЕТОД АУТЕНТИФІКАЦІЇ ПАКЕТУ ОНОВЛЕННЯ ДІАГНОСТИЧНИХ ПАРАМАТРІВ АВТОМОБІЛІВ

Водоп'янов Арсеній Володимирович, здобувач вищої освіти
Національний університет біоресурсів і природокористування України

Аутентифікація для пакету оновлення потрібна головним чином для забезпечення надійності його джерел та для запобігання ненадійним установам надсилати пакет оновлення на платформу автомобіля [1].

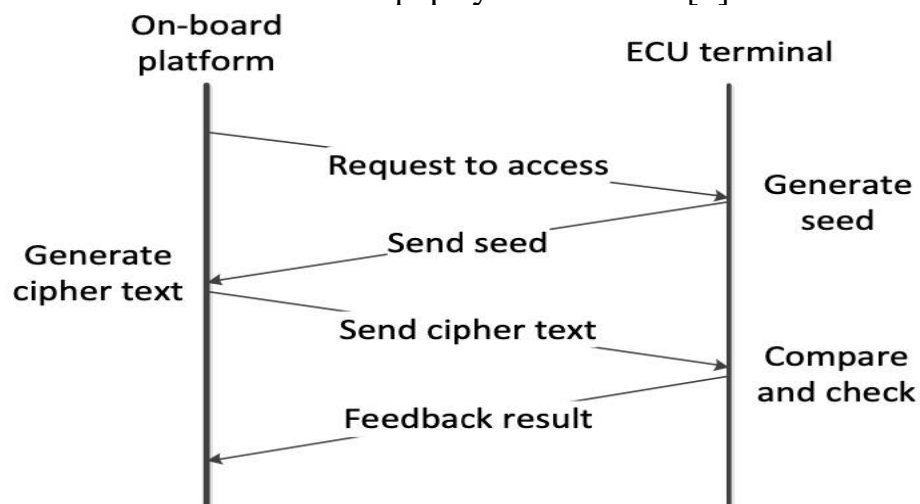


Рис. 1 – Процес перевірки безпеки

Перевірка цілісності даних дозволяє перевірити, чи були дані підроблені чи ні, і переконатися, що файл, завантажений на платформу автомобіля, є ефективним пакетом оновлення ECU. На рис. 1 показано процес автентифікації та перевірки цілісності пакету оновлення на основі алгоритму цифрового підпису RSA.

Сторона сервера: по-перше, пакет оновлень хешований, щоб сформувати анотацію інформації про оновлений файл. Потім анотація та секретний ключ сервера використовуються для генерації підпису алгоритмом генерації підписів RSA. Нарешті, підпис та пакет оновлень надсилаються на платформу автомобіля.

Сторона платформи транспортного засобу: після отримання пакету оновлення та підпису від сервера, відкритий ключ сервера застосовується для перевірки через алгоритм RSA.

Дійсний підпис означає, що пакет оновлення є приватним ключем сервера, який є надійним джерелом. Потім її цілісність додатково перевіряється. Якщо він не пошкоджений, файл буде збережено.

Відповідно до положень розділу оновлення ECU в діагностичному протоколі LAN контролю дорожнього руху (ISO 15765), безпечний доступ вказаний як рекомендований етап оновлення ЕБУ автомобіля. Положення протоколу загальної діагностики поломок транспортного засобу ISO 14299 (ISO 14299) про службу безпеки забезпечують базовий процес оновлення ЕБУ. Механізм захисту доступу в цьому документі базується на ISO 14299, як показано на рис. 1. Включаються наступні кроки:

1. Комп'ютер платформи автомобіля запитує доступ до ECU.
2. Термінал ECU автомобіля генерує випадкове ядро і відправляє його на платформу транспортного засобу. У той же час ECU використовує ключ та код як вхідні дані для обчислення тексту шифру за узгодженим алгоритмом шифрування.
3. Комп'ютер платформи транспортного засобу приймає програмний код. Потім програмне забезпечення шифрується за тим самим алгоритмом та ключем, щоб отримати текст шифру. Далі текст шифру надсилатиметься в ECU у автомобіля.
4. ECU порівнює текст шифру з платформи автомобіля та текст шифру, сформований у кроці 2. Узгоджені ключі означають, що запитуючий пристрій має узгоджений ключ і знає алгоритм шифрування ключа, термінал ECU є законним, тому ECU буде розблоковано. В іншому випадку ЕБУ заборонить доступ.
5. Результат надсилається на платформу транспортного засобу.

Література

1. Hryniv A., Rogovskii I., Aulin V., Lysenko S., Titova L., Zagurskiy O., Kolosok I. Development of a system for determining the informativeness of the diagnosing parameters of the cylinder-piston group of the diesel engines in operation. Eastern-European Journal of Enterprise Technologies. 2020. Vol. 3 (5 (105)). P. 19–29. doi: 10.15587/1729-4061.2020.206073.

Міністерство
освіти і науки
України



Міністерство освіти і науки України

Національний університет біоресурсів і
природокористування України

Механіко-технологічний факультет

Кафедра транспортних технологій та засобів у АПК

Академія прикладних наук Університету
управління та адміністрування в Ополі

Академія інженерних наук України
Українська асоціація аграрних інженерів



**ЗБІРНИК ТЕЗ
доповідей
VIII Міжнародної
науково-практичної конференції
«Автомобільний транспорт та інфраструктура»**



AutoTransport and Infrastructure

**17-19 квітня 2025 року
м. Київ**

УДК 631.17+62-52-631.3

Рекомендовано до друку рішенням вченої ради механіко-технологічного факультету Національного університету біоресурсів і природокористування України від 20 травня 2025 р., протокол №. 12

Збірник тез доповідей VIII Міжнародної науково-практичної конференції «Автомобільний транспорт та інфраструктура» (17–19 квітня 2025 року). Національний університет біоресурсів і природокористування України. Київ. 2025. 242 с.

ISBN 978-617-8530-21-1

В збірнику представлені тези доповідей науково-педагогічних працівників, наукових співробітників, докторантів і аспірантів, студентів, фахівців транспортної галузі, учасників VIII Міжнародної науково-практичної конференції «Автомобільний транспорт та інфраструктура», в яких розглядаються нинішній стан та шляхи розвитку автотранспортної галузі.

ISBN 978-617-8530-21-1

© НУБіП України, 2025.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ:

Тонха О.Л., проректор з наукової роботи та інноваційної діяльності НУБіП України – голова організаційного комітету;

Отченашко В.В., начальник науково-дослідної частини НУБіП України – заступник голови організаційного комітету;

Братішко В. В., декан механіко-технологічного факультету НУБіП України – заступник голови організаційного комітету;

Киричок П.О., президент Академії інженерних наук України – заступник голови організаційного комітету (за згодою);

Тадеуш Покуса, проректор Академії прикладних наук Університету управління та адміністрування в Ополь (Польща) – співголова організаційного комітету (за згодою);

Ілесалієв Д. І., ректор Ташкентського Перфектного університету (Узбекистан) – співголова організаційного комітету (за згодою);

Дашдаміров Ф.С., директор Інституту логістики і транспорту Азербайджанського технічного університету (Азербайджан) – співголова організаційного комітету (за згодою);

Загурський О.М., професор кафедри транспортних технологій та засобів у АПК НУБіП України – секретар організаційного комітету.

Дьомін О.А., доцент кафедри транспортних технологій та засобів у АПК НУБіП України;

Калінін Є. І., завідувач кафедри тракторів та автомобілів НУБіП України;

Мацюк В. І., професор кафедри транспортних технологій та засобів у АПК НУБіП України;

Умідулла Абдураззоков, завідувач кафедри транспортної техніки Ташкентського державного університету транспорту (Узбекистан);

Роговський І. Л., завідувач кафедри технічного сервісу та інженерного менеджменту імені М. П. Момотенка НУБіП України;

Павло Навицький, професор університету Орала Робертса (США);

Савченко Л.А., завідувачка кафедри транспортних технологій та засобів у АПК НУБіП України;

Софі Лю, професор Університету Орала Робертса (США);

Степанов О.В. заступник декана з наукової роботи механіко-технологічного факультету НУБіП України.