Fleet cards, Fuel cards - Transition from 3DES to AES

Martin Rupp

SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

In this article, we shall describe how fleet fuel cards should be transitioned from 3DEs to AES.

An overlook at Fuel cards

Fuel cards are issued by special companies such as Wex Inc, Fuelman or Comdata, for example. Additionally, they can also be issued by banks following a credit card payment scheme (Visa, MasterCard,...)

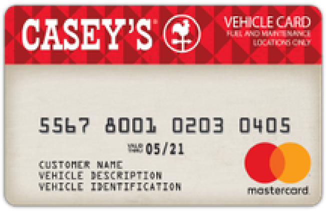
Fleet fuel cards allow company employees to purchase fuel and repair services inside a network of partner gas stations (usually most of the gas stations in the US accept these cards) and other merchants.

The fleet operator of a company can monitor transactions and make sure there is no fraud or that cards are wrongly used for other purposes. Additionally Fleet Fuel cards often offer interesting rebates and loyalty programs.

Here we list the most important non-bank fuel card issuers

Brand Fleet Fuel Card Issuer		**description**

CEFCO		Mastercard branded fuel card
WEX		Proprietary payment network fuel card Wex offers a wide variety of fuel cards and acts as well as a brand
SPEEDWAY		Proprietary payment network fuel card Can be Wex branded “Accepted at all Speedway locations. Plus, additional acceptance at 95% of retail fuel locations and 45,000 service locations throughout the U.S”
FUELMAN		Proprietary payment network fuel card “40,000+ stations nationwide on the Fuelman Discount Network”

		  Fuelman 556701 52645 485145 VEHICLE ID COMPANY LLC 012345 EXP 08/22 Also offers Mastercard branded fuel cards (‘Universal’ cards) UNIVERSAL PREMIUM FLEET CARD MULTI 5567 9134 5678 9012 12/17 JOHN Q SMITH ABC CORPORATION MasterCard
[ARCO]()	ARCO	Mastercard branded fuel card ARCO Business Solutions Universal Fuels Management CORPORATE FLEET 5567 8001 0203 0405 09/18 JOHN Q. CUSTOMER ABC COMPANY MasterCard
[CASEY’s]()	CASEY'S GENERAL STORE	Mastercard branded fuel card  CASEY'S VEHICLE CARD FUEL AND MAINTENANCE LOCATIONS ONLY 5567 8001 0203 0405 05/21 CUSTOMER NAME VEHICLE DESCRIPTION VEHICLE IDENTIFICATION mastercard
[SHELL]()	Shell	Proprietary payment network fuel card issued by the oil company Shell Shell Card VALID IN EUROPE 7002001234567890123 PROFESSIONAL FLEET 3 EUROPE A CUSTOMER 12/21

BP	bp	Proprietary payment network fuel card issued by the oil company British Petroleum (B.P) bp ARAL BP + Aral Routex 123456 789012 123456 EU.EUROPE M.EUROPE INT0012/20
KWIK TRIP	KWIK TRIP	Offers both proprietary payment network fuel card and Mastercard branded fuel card Kwik Trip Extended Fleet 707649 99260 083927 CUSTOMER BUSINESS NAME VEHICLE DESCRIPTION VEHICLE NUMBER EXP 11/18 Kwik Trip Business Plus FLEET 5567 8001 0203 0405 5567 VALID THRU 09/14 JOHN Q. CUSTOMER ABC COMPANY MasterCard
COMDATA	COMDATA	proprietary payment network fuel card COMDATA 5523 4523 4567 8901 5523 ABC COMPANY VALID THRU 01/18
PETROL PLUS	ппр передовые платежные решения	proprietary payment network fuel card (Russia) ВЕЗДЕХОД Online Петрол Плюс 8 (800) 5555 200 VALID THRU 12/20 1234 567890

Fleet Fuel Cards aren’t payment cards nevertheless they require high security all the same

Fuel cards are not payment cards such as cards issued by banks and cards branded by Mastercard or Visa and operating in a payment network. Instead, they operate in a private loop whose implementation will vary with the card issuer.

Nevertheless, they require equivalent - if not superior - security as their bank equivalent. They need messaging authentication as many of these cards are using the ISO 8583 messaging standards. They also often use an ‘EMV-like’ system with cryptograms and their own certification authority inside a proprietary payment network.

Here we summarize the four possible types of fuel cards:

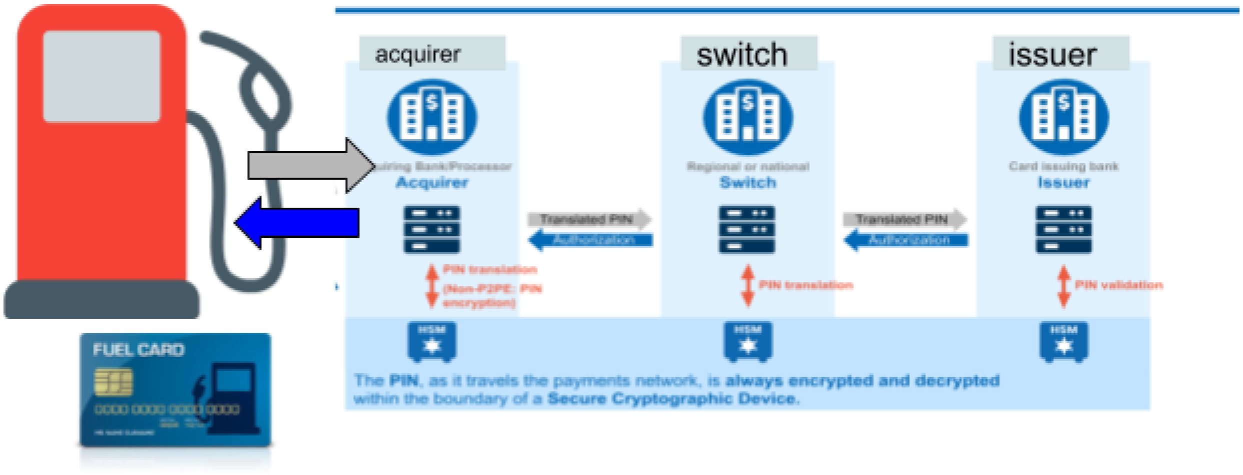
	PCI-DSS (Payment networks)	**With EMV**
Proprietary norm Proprietary payment network fuel card	no	no
EMV fuel card	no	yes
Payment fuel card (magstripe)	yes	no
EMV payment fuel card (chip)	yes	yes

Some fuel card issuers may issue different card types: for example, a MasterCard chip-less fuel card which operates in PCI-DSS infrastructure but is not EMV or a chip-based fuel card which is using a proprietary network.

In all cases, the fuel cards require high security and often use key blocks to translate information from one zone to another.

Next, we represent how the PIN, for example, is often encrypted inside key blocks and travel through zones via PIN translation mechanisms where HSMs securely translate such data at each frontier between two zones.

The Fuel Card payment Network



Why Fuel Cards must migrate from triple-DES to AES

Fuel cards that are using cryptography most often use banking protocols and norms, slightly modified if they use their own proprietary systems. Nevertheless, Fuel card issuers that are using 3DES should migrate their system to AES.

There are many reasons for this.

- Triple DES uses keys which have an effective strength of 2x56=112 bits, which is considered to be slightly small with today’s capacity for computing power;

- Triple DES relies on single DES - which is broken. Therefore a Triple-DES key which could be broken into two sub-DES keys with two corresponding ciphertexts would be as well broken;
- AES is considered to be better in general, it has a bigger capacity than offers longer crypto periods
- NIST officially deprecated 3DES and supports AES as an encryption standard scheme

The AES-DUKPT key derivation scheme should be also recommended for fuel cards. It is faster and more secure than the Triple-DES DUKPT.