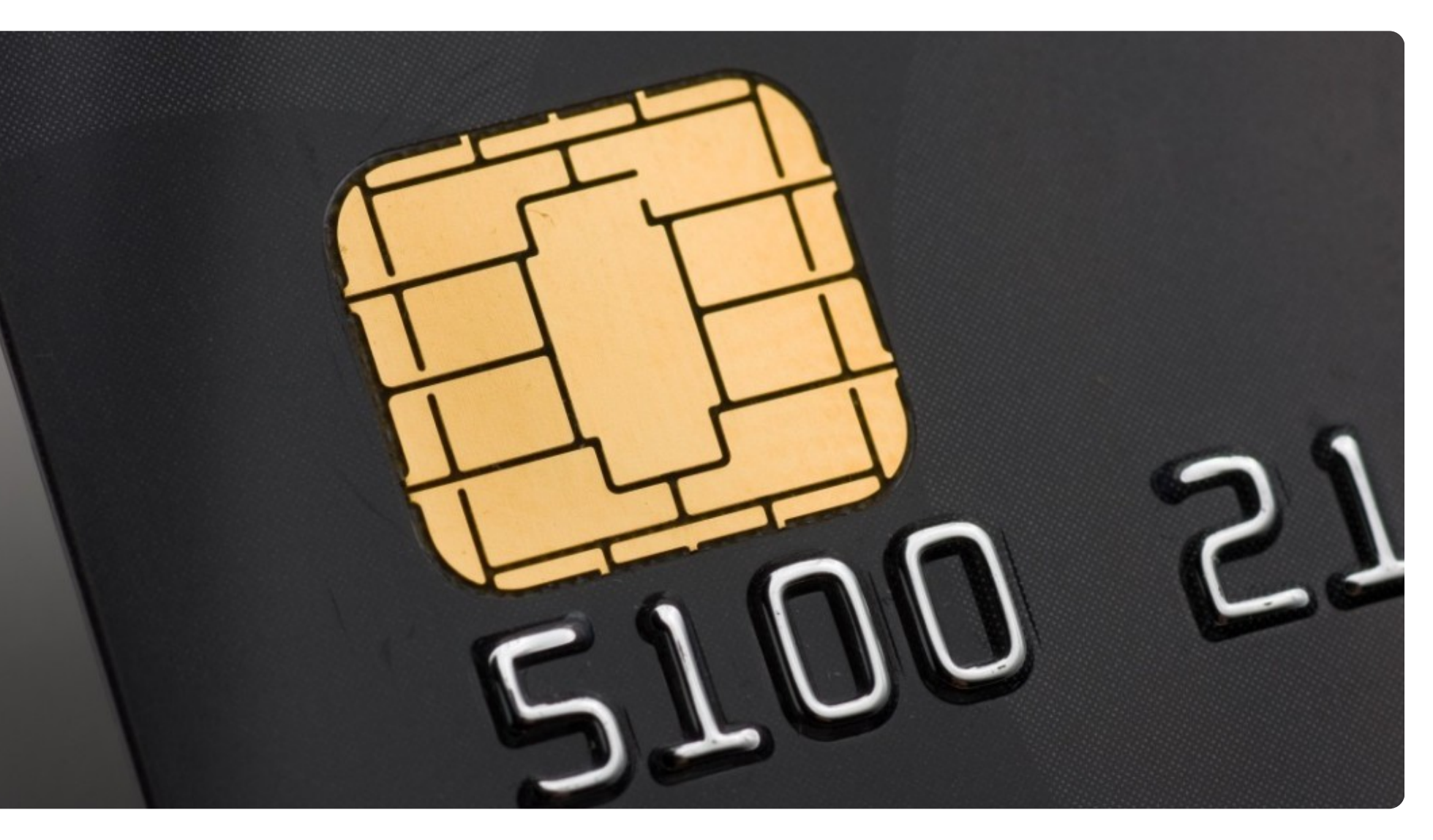

EMV Application Specification :: Offline Data Authentication (ODA) - part I

Ahmed Hemdan Farghaly
Senior Manager | Fintech | EFTPOS | mPOS | ISO8583 | EMV | NFC | QR | PCI-DSS | PA-DSS

Veröffentlicht: 23. Feb. 2022

Static Data Authentication (SDA)

Going a step further, We'll talk about Offline Data Authentication and the different methods used, and how it is one of the important steps in the EMV transaction journey.

Please refer to the previous article about Read Application Data: here

Offline data authentication is a cryptographic check to validate the card authenticity.

It basically makes use of the RSA algorithm which is an asymmetric cryptography algorithm uses a pair of keys public and private to perform the encryption/decryption process.

There is a nice article about it here:

https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

If we recall from previous article, the card responds to GPO was:

Application File Locator [AFL] [tag 94] which is the list of files and records that the terminal shall read from the card, some of these data will be marked to be used in the ODA process.

Application Interchange Profile [AIP] [tag 82] which is the supported functions by the card that the terminal needs to perform along the transaction flow.

>> referring to EMV 4.3 Book 3 Table 37: Application Interchange Profile. Here, Byte 1 in AIP will indicate the ODA method(s) supported by the card.

The rule here is: If the terminal and the ICC support a common method for Offline Data Authentication, the terminal shall perform Offline Data Authentication.

There are 3 ODA methods: (we'll talk about each method in details)

Combined Dynamic Data Authentication CDA (strongest).

Dynamic Data Authentication DDA.

Static Data Authentication SDA.

And in that case the priority of choosing which method to perform will be:

- If both terminal and card support CDA, terminal shall perform CDA.
- Else if both terminal and card support DDA, terminal shall perform DDA.
- Else if both terminal and card support SDA, terminal shall perform SDA.
- If none of the above, terminal shall set the 'Offline data authentication was not performed' bit in the TVR to 1.

A new concept starts to appear here:

- Terminal Verification Result (TVR): An EMV data object which consists of a series of bits set by the terminal during EMV transaction flow, and later on used to form the terminal's decision whether to accept, decline or go on-line for authorization.

It consists of 5 bytes where each bit will have a specific meaning.

>> referring to EMV 4.3 Book 3 Table 42: Terminal Verification Results

- Terminal Status Information (TSI): Another data object set by the terminal during EMV transaction flow indicating the functions that have been done during EMV transaction flow.

It consists of 2 bytes, one of them actually has specific meanings, the other one is RFU.

>> referring to EMV 4.3 Book 3 Table 43: Transaction Status Information.

Static Data Authentication (SDA): explained

SDA is used to confirm the legitimacy of critical ICC-resident static data.

EMV 4.3 Book 2: Figure 1: Diagram of SDA

The process usually requires data generated by the issuer, and terminal validating the data somehow.

If the terminal failed in one of the following steps, terminal shall set the 'SDA failed' bit in the TVR to 1 (B1b7).

Here are the steps to perform a proper SDA. In our example, we'll use RID=A000000003 and Index=95 for VISA test card.

The card::

- Issuer generates key pair (issuer public and private key).
- The network [i.e. VISA] signs this issuer public key and generates a certificate (Issuer PK Certificate).
- Store the Issuer PK Certificate on the card [tag 90].
- Store the public key index for the key pair that was used by the network to sign the issuer public key. (i.e. PKI 95 for visa test card) [tag 8F].
- Issuer creates a certificate containing a signature on important card data (signed static app data SSAD) and store that certificate on the card [tag 93].

The terminal::

- Terminal retrieves the PKI stored on the card [tag 8F].

8F Certification Authority Public Key Index "95"

- Terminal loads the CA public key for that index (terminal should have a way of storing and loading all supported CAPKs for all the supported RIDs).

Key Modulus: "BE9E1FA5E9A803852999C4AB432DB28600DCD9DAB76DFAAA47355A0FE37B1508AC6BF38860D3C6C2E5B12A3CAAF2A7005A7241EBAA7771112C74CF9A0634652FBCA0E5980C54A64761EA101A114E0F0B5572ADD57D010B7C9C887E104CA4EE1272DA66D997B9A90B5A6D624AB6C57E73C8F919000EB5F684898EF8C3DBEFB330C62660BED88EA78E909AFF05F6DA627B" *Exponent:* "03"

- Terminal retrieves Issuer Public Key Certificate [tag 90], Issuer Public Key Reminder if any [tag 92], and Issuer Public Key Exponent [tag 9F32]

90 IssuerPKCert "8B3901F6253048A8B2CB08974A4245D90E1F0C4A2A69BCA469615A71DB21EE7B3AA94200CFAEDCD6F0A7D9AD0BF79213B6A418D7A49D234E5C9715C9140D87940F2E04D6971F4A204C927A455D4F8FC0D6402A79A1CE05AA3A526867329853F5AC2FEB3C6F59FF6C453A7245E39D73451461725795ED73097099963B82EBF7203C1F78A529140C182DBBE6B42AE00C02"

92 Issuer Public Key Remainder "33F5E4447D4A32E5936E5A1339329BB4E8DD8BF0044CE4428E24D0866FAEFD2348809D71"

9F32 Issuer Public Key Exponent "03"

- Terminal decrypts the issuer public key certificate using CA public key.

Decrypted IssuerPKCert "6A02476173FF121500405401019001A687AF619B88CBAD371903C89579B5890D605F905B093C1F856801AE33C12E65D02B64454D9921468283ED397835909BCBB2F659460833BAAC1C75343FF671EB93F04953C6AEF428F07EE28FC9ABFB65CF6A961B4A085AF297CD1453CF4719868883D20A8F624E45920BA3C98C5453DBF74927FD240C07C4262F736E460BB5FABC"

Refer to EMV 4.3 Book 2 Table 6 for the format of data recovered from issuer public key certificate.

- Validate the recovered data against that format to make sure it is correct.
- Extract Issuer Public Key (append Issuer Public Key Reminder if any).

From the above IssuerPKCert, we can extract the Issuer Public Key (or part of it) and append Issuer Public Key Reminder if any.

Here we have only part of it: "A687AF619B88CBAD371903C89579B5890D605F905B093C1F856801AE33C12E65D02B64454D9921468283ED397835909BCBB2F659460833BAAC1C75343FF671EB93F04953C6AEF428F07EE28FC9ABFB65CF6A961B4A085AF297CD1453CF4719868883D20A8F624E45920BA3C9"

After appending the Issuer Public Key Reminder.

Full IssuerPK: "A687AF619B88CBAD371903C89579B5890D605F905B093C1F856801AE33C12E65D02B64454D9921468283ED397835909BCBB2F659460833BAAC1C75343FF671EB93F04953C6AEF428F07EE28FC9ABFB65CF6A961B4A085AF297CD1453CF4719868883D20A8F624E45920BA3C933F5E4447D4A32E5936E5A1339329BB4E8DD8BF0044CE4428E24D0866FAEFD2348809D71"

- Terminal retrieves the Signed Static App Data [tag 93].

93 Signed Static Application Data "8F48E691403494057688B22B237EF0EE40238539BB9DE99A97DC2C47B3427F292651BF538BB89C046F86CE05C5578CC12007F3D4F8436847662DF78CB385AFB815B7E28097C0A520F67D4267A3531E6C7CEB7610B113A369C0D5892515FE062BF7BA16DA57C04095245007E1B38B7823B9AB4A5177A18348AD4CE7A8E99F4404C256B4061286794D8B41B2CF42E4022B"

- Terminal decrypts the certificate using the issuer public key.

Decrypted Signed Data:: "6A0301DAC5BBC54A4F8658F9433490D1929B182D8D5D56D8DD57BC"

Refer to EMV 4.3 Book 2 table 7 for the format of data recovered from signed static app data.

- Validate the recovered data against that format to make sure it is correct.
- Extract the hash result [signature made on the static app data] we'll need it later to compare.

Signed data hash 1: "C54A4F8658F9433490D1929B182D8D5D56D8DD57"

- Using the SHA-1 algorithm, the terminal will create a signature on the data that is read as part of the read card data step which was marked to be used in the ODA process.
- Build a block of data following EMV 4.3 Book 2 table 3.

Signed Data: "5A0847617390010101195F340101" (from read data step)

Signed Data Block:: "0301DAC5BB5A0847617390010101195F340101"

- Compute a signature for this block of data (using SHA-1).

Signed data hash 2: "C54A4F8658F9433490D1929B182D8D5D56D8DD57"

- Compare the 2 signatures and if they are equal, that means the data is authentic, and SDA was successful.
- The terminal shall set the 'Offline data authentication was performed' bit in the TSI to 1 (B1b8).

Up next… Dynamic Data Authentication DDA.

Weitere Artikel von dieser Person

Ebenfalls angesehen