Online Dynamic Authentication

**Introduction**

Online dynamic authentication is the process, which guarantees the mutual authentication between the card and the issuer during online processing.

This action performed by the acquirer or issuer systems are outside the scope of EMV specification. However, an explanation of what is expected to take place at the issuer may be useful for clarity. The online dynamic authentication is split in two parts: the online card authentication and the online issuer authentication.

The ARQC is a cryptogram generated by the card from transaction data using a secret key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby authenticate the card. This process is termed ‘online card authentication’ or simply ‘card authentication’.

Subsequent to card authentication, the issuer may generate a cryptogram on selected data included in the authorisation response or already known to the card. This cryptogram is sent to the terminal in the authorisation response as part of the Issuer Authentication Data (IAD). The terminal provides the Issuer Authentication Data to the card. The card may use the Issuer Authentication Data to authenticate that the response message originated from the issuer. This process is called ‘online issuer authentication’.

**Card and issuer authentication related data exchange**

**References**

- [Visa Appl] Visa Integrated Circuit Card - Application Overview - Version 1.4.0
- [Visa Terminal] Visa Integrated Circuit Card - Terminal Specification - Version 1.4.0

**Note about this White Paper**

EMV 4.1 Book 2 provides in section 8 methods for the generation of the Authorisation Request Cryptogram (ARQC) generated by the card and the Authorisation Response Cryptogram (ARPC) generated by the issuer and verified by the card. Issuers may decide to adopt other methods for these functions. Unless indicated otherwise the descriptions hereafter follows the EMV recommendations. For clarity, the algorithms described here may have been simplified.

**Online Card Authentication**

The issuer performs online card authentication during an online authorization, using Message Authentication Code cryptography (MAC). The card calculates a cryptogram, called the ARQC, which is sent to the issuer as part of the
authorization request. The issuer can use its own copy of the card secret key to check that the cryptogram is valid, and therefore that the card is genuine (since only a genuine card will know the correct secret key).

ARQC algorithm simplified:

**Transaction Data** = Amount, Currency, PAN, Date, Time, Transaction Counter, Unpredictable Number...

**ARQC** = MAC(Card secret key, Transaction Data)

The issuer host dynamically authenticates the card in the following manner:

- The card requests data items from the terminal. These items will include the transaction amount, currency, unpredictable number...
- The card uses its secret card master key with which it was loaded by the issuer at personalization time, and a session key derivation algorithm, to produce a session key. This session key will be specific to this transaction.
- The card uses this session key to generate the ARQC by applying the MAC algorithm over a subset of the transaction data (terminal and card data). This ARQC is sent to the terminal together with the card data used for its calculation.
- The terminal sends the data and the ARQC to the issuer host.

When the issuer receives the authorization request, with the card related data and ARQC, it can verify the MAC as follows:

- The issuer host, using the secret issuer master key and a card key derivation algorithm, recovers the card master key.
- The issuer host computes the session key that the card used to generate the ARQC.
- The issuer host system uses this regenerated session key, and the cleartext transaction data it received, to recalculate the ARQC.
- If the recalculated ARQC is the same as the one received from the card, the issuer host can be sure that the card is genuine (since it knows the secret card master key) and that the transaction data it is being asked to authorize has not been altered (since changing the data would invalidate the ARQC).

For more details:

- The EMV recommended minimum set of data elements for ARQC generation is given in Table 25 of [EMV Book 2].
- MasterCard recommends to use the EMV minimum set of data elements for ARQC generation plus the proprietary data "Card Verification Results" cf. Table 4.1 of [MC Security].
- Visa recommends the same data as MasterCard for generating ARQC. cf Table D-1 in [Visa Card].
- The EMV recommended session key derivation algorithm is described in Annex A.1.3 of [EMV Book 2].
- MasterCard recommends the EMV session key derivation algorithm but the M/Chip 2.1 derivation method may be used. The M/Chip 2.1 method is described in Chapter 7 page 7-4 of [MC Security].
- The MAC algorithm is specified in Annex A.1.2 of [EMV Book 2]. Both MasterCard and Visa use it.
- See [EMV Book 2] Annex A.1.4 for EMV recommended master key derivation algorithms. MasterCard and Visa recommend using the EMV master key derivation algorithms.

Online card authentication with a chip card has the advantage that it is dynamic – that is to say the cryptogram that the card computes is different for each transaction and so cannot be replayed. It ensures the presence of the card during the transaction, protects the issuer against altered cards, counterfeited cards and ensures the integrity of the transaction data communicated to the issuer.

**Online Issuer Authentication**
In the online response, the issuer host includes the Issuer Authentication Data (IAD) where the issuer provides the Authorization Response Cryptogram (ARPC) to allow the card to authenticate its own issuer as the sender of the response. The card can ensure that the authorization response has come from the genuine issuer by checking the IAD. If the IAD can be correctly validated, the card has proof that the response came from the genuine issuer. The card can therefore execute the instructions received in the online response.

The structure of the Issuer Authentication Data is proprietary to the issuer. But it is normally composed of two parts:

- **Issuer information**, instructing the card to:
  - Accept or decline the transaction.
  - Reset card internal counters
  - ...
- **The Application Response Cryptogram (ARPC)** calculated by the issuer, proving to the card that the instruction comes from the genuine issuer.

**Simplified Issuer Authentication Data generation:**

\[
\text{ARPC Response Code} = \text{informs the application about the actions decided by the issuer.}
\]

\[
\text{ARPC} = \text{GenerateARPC(Card secret Key, ARPC Response Code, ARQC)}
\]

\[
\text{IAD} = \text{ARPC, ARPC Response Code}
\]

The card dynamically authenticates the issuer host in the following manner:

- The issuer generates the card specific Authorisation Response Code (ARC) indicating its decision to accept or decline the transaction.
- The issuer host, using the secret issuer master key and a card key derivation algorithm, recovers the card master key.
- The issuer host computes the session key to generate the ARPC. This session key will be specific to this transaction.
- The issuer host system uses this session key, the ARPC Response Code and the ARQC it received, to compute the ARPC.
- The issuer generates the IAD using the ARPC and the ARPC Response Code.
- The IAD is sent to the terminal and the terminal transmits it to the card.

When the terminal receives the authorization response with the IAD, the card can verify the ARPC as follows:

- The card retrieves the ARPC and the ARPC Response Code from the IAD.
- The card uses its secret card master key with which it was loaded by the issuer at personalization time, and a session key derivation algorithm, to recalculate the session key used by the issuer.
- The card uses this session key to generate the ARPC by applying the ARPC algorithm over ARPC Response Code and ARQC (this last data is kept internally by the card since its generation).
- If the recalculated ARPC is the same as the one received from the issuer host system, the card can be sure that the issuer host is genuine (since it knows the secret card master key) and that the issuer host decision has not been altered (since changing the decision would invalidate the ARPC).
- The card will accept or decline the transaction according to the host decision and its internal logic.

For more details about the algorithms used for the ARPC generation, you can find the two EMV recommended methods for ARPC generation in [EMV Book 2] section 8.2.1 and 8.2.2.

Online issuer authentication with a chip card has the advantage that it is dynamic – that is to say the cryptogram that the issuer host computes is different for each transaction and so cannot be replayed. It ensures the issuer decision, protects the card against fake issuer and ensures the integrity of the communication from the issuer host system.

**Online Issuer Authentication**
Conclusion

Online dynamic authentication offers a strong mutual authentication and a strong protection against communication alteration between the card and the issuer host.

Glossary

<table>
<thead>
<tr>
<th>ARC</th>
<th>Authorisation Response Code: The issuer’s answer to an authorisation request. The issuer’s responses are typically: approve the transaction, decline the transaction, call your bank...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARQC</td>
<td>Authorisation Request Cryptogram: The cryptogram generated by the card for transactions requiring online authorization and sent to the issuer in the authorization request. The issuer validates the ARQC during the online card authentication process to ensure that the card is authentic, was not created using skimmed data and that data stored in the card has not been altered since card issuance.</td>
</tr>
<tr>
<td>ARPC</td>
<td>Authorisation Response Cryptogram: A cryptogram generated by the issuer and sent to the card in the authorization response. This cryptogram is the result of the Authorization Request Cryptogram (ARQC) and the issuer’s authorization response code (ARC) encrypted with the card secret key. The cards validates it during online issuer authentication to ensure that the response came from a valid issuer.&lt;&lt;&lt;&gt;&gt;&gt;</td>
</tr>
<tr>
<td>ARPC Response Code</td>
<td>The ARPC Response Code informs the application about the actions decided by the issuer. The ARPC Response Code is sent to the application in the Issuer Authentication Data (last two bytes). It replaces the Issuer Authentication Response Code in previous versions of EPI/MCI Implementation Specifications for Debit and Credit.</td>
</tr>
<tr>
<td>Authentication</td>
<td>A cryptographic process that validates the integrity of data and its origin.</td>
</tr>
<tr>
<td>Card master keys</td>
<td>These keys are used to generate session keys unique for each transaction. The card uses these session keys to compute ARQCs and validate issuer’s ARPCs.</td>
</tr>
<tr>
<td>Cryptogram</td>
<td>A numeric value that is the result of data elements put into an algorithm and then encrypted. It is commonly used to validate data integrity.</td>
</tr>
<tr>
<td>IAD</td>
<td>Issuer Authentication Data: Data sent to the card from the issuer host for online issuer authentication.</td>
</tr>
<tr>
<td>Issuer master keys</td>
<td>These keys are used to generate the unique card master keys for each card during personalisation. The issuer hosts uses them to recover the card master keys to validate ARQCs and generate ARPCs.</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code: A numeric value generated using a cryptographic algorithm, which establishes that the contents of a message have not been changed and that the message was generated by an authorized entity.</td>
</tr>
<tr>
<td>Session Key</td>
<td>A temporary cryptographic key computed and no longer valid after the end of the transaction.</td>
</tr>
</tbody>
</table>