

# AUTHENTIC AUTHORIZATION RULES

***A powerful feature of Authentic and Authentic Gateway is their so-called Authorization Rules capability, which enables users with no programming knowledge rapidly to create and deploy rules to refer or decline transactions, rules. This Authorization Rules capability represents a radical departure from the hard coded, programmatic approach so familiar in competitive products.***

Authorisation Rules can be applied in different ways:

- As a pre-authorisation prior to routing a transaction out to an issuer or network for further authorisation
- As a stand-in authorisation when an issuer or network cannot be reached
- As a full authorisation accessing card and account details

There are many different types of authorisation rule available in Authentic and Authentic Gateway, as follows.

## **Card Authentication Rules**

These are used to identify the cardholder, and include rules such as: card on file, card verification value (cvv) correct, cvv2 (the three digit code written on the card), PIN correct, valid ARQC (for chip transactions), valid expiry and issue date. Card Authentication Rules reduce the possibility that the card is fraudulent. The ARQC validation for chip cards dramatically increases the probability that the card is genuine, but this is only available where the chip details have been read.

## **Card usage rules**

These limit the cardholder's use of the card, for example checking that the transaction is valid for a given type of card (perhaps using the service code on the track data), enforcing domestic and foreign ATM limits, checking the card status on file for refer, decline or pickup card response to a transaction.

Card status values can cause a rule to be executed - for example, a status on a card could invoke a rule that the cardholder is not allowed domestic ATM transactions.

## **Checking for Available funds**

Authentic supports sufficient funds checking for different types of card, including debit cards, pre-paid cards, charge cards and credit cards.

For debit cards, transactions can be authorised to an overdraft limit or a minimum balance.

For pre-paid cards, transactions can never allow the card to exceed the pre-paid amount, even if an additional amount is guaranteed with a transaction.

For example, a restaurant charge may guarantee a tip of 15%. For a credit card, the cardholder may be allowed to exceed the credit limit by a percentage or use only a part of the credit limit depending on factors such as the type of transaction, the type of merchant, the length of time as a cardholder, the amount of the transaction, the country in which the transaction is made, and other conditions configurable by the card issuer.

The credit risk can be managed for a single card, or a group of

related cards using a single account. A family relationship, where the parents have a joint credit limit and each child has a monthly limit subject to available funds in the parents account, is also supported.

The results of credit limit checking can be used to change the offline limits on a chip card. For example, if a cardholder is close to the credit limit, the offline parameters can be reduced, making the card come on line more frequently.

## **Restricting fraud.**

As fraud continues to grow, issuers and acquirers continue to develop strategies to detect fraud.

Within Authentic, rules that identify known fraudulent sequences can be applied, with a decline, refer or approve result code. An alert can also be raised. The rules to achieve this are created through configuration screens.

Many fields in the transaction can be tested, and historic transactions for the card or merchant can be compared.

For example, a simple rule could decline if there are more than three transactions in an hour by a cardholder in a jewellery store. A more complex rule could be: decline if a low value authorisation at a telephone kiosk in the USA is followed some time later by an authorisation for electrical goods in Spain. As fraud patterns emerge, the user can input rules to prevent or alert these sequences of transactions.

The results of fraud risk checking can also be used to change the offline limits on a chip card. For example, the



offline limits can be lowered if the card is used in a high risk country.

**Authorisation Rule Configuration**

The authorisation rules which Authentic uses to process a transaction are identified from the following elements:

- The card identifier, extracted from digits in the card number (PAN). Usually the first few digits of the PAN identify the card type, but sometimes other digits can be used as well. Authentic can group cards with different card identifiers into a single set of authorisation rules.
- The card product code held on the Authentic database. Sometimes an Issuer will have several different types of card all with the same card identifier. A product code allows different rules to be set up for the different card types.
- The transaction type. Separate authorisation rules

can be set up for different types of transaction, such as balance enquiry, purchase cash withdrawal.

Authorisation rules are configured via a GUI and new rules can be added without changing existing code. The configuration screens allow a new rule to be included in one or more authorisation lists.

A fundamental tenet in the design of Authentic is that customisation should be achievable by configuration rather than coding, to the greatest extent possible.

Most conceivable rules can be configured without writing code, particularly rules for checking available funds, rules for imposing spending limits like the ATM daily limit, and rules for detecting known fraud patterns.

For example, configuration screens allow a rule to be generated that:

- Selects particular values in a transaction, such as a particular country, or a type

of merchant, or a large amount, and totals the number or total value of these transactions for a cardholder or merchant in a period such as a day.

- Selects values in previous transactions that are indicators of fraud in the current transaction. Low value transactions through petrol stations or telephone kiosks often increase the risk of subsequent transactions being fraudulent.

If a specific requirement cannot be met by pure configuration, it is a simple task to create a new Java code snippet for point-&-click configuration into authorisation rules via the rules GUI.

**Fraud prevention and risk management**

Authentic’s authorisation rules provide users with powerful and dynamic means of responding rapidly to evolving credit and fraud risk events.

