Decrypting Realtime Authorization Events

`REALTIME_AUTH_EVENTS` = the set of messages related to card authorization events.

Spec = **ISO 8583**

> **ISO 8583** is an international standard for *financial transaction card originated* interchange messaging.

see also: Transaction Data 💱 + https://chime.atlassian.net/wiki/spaces/~230762622/pages/1482591746 Request access

---

Most of the information on this page is further defined in the Galileo Auth API 2.0 documentation found here.

The information on this page is ordered as it is viewed in Admin (example).

Field	Description	Data Table - Field Name
ID	Unique transaction identification key generated by Chime	`edw_db.core.fct_realtime_auth_event` - `auth_event_id`

Created At	Timestamp of the transaction (PST)	`edw_db.core.fct_realtime_auth_event` - `auth_event_created_ts`
		`edw_db.core.fct_authorized_transaction` - `transaction_timestamp`
		`mysql_db.chime_prod.alert_authorization_events` - `created_at`
		• NOTE: timestamp is GMT

Updated At	Generally the same as the **Created At** field; can be different if original API call	`edw_db.core.fct_realtime_auth_event` -

	failed	`auth_event_updated_ts`
		`mysql_db.chime_prod.alert_authorization_events` - `updated_at`
		• NOTE: timestamp is GMT

User	Unique user identification key generated by Chime	`edw_db.core.fct_realtime_auth_event` - `user_id`
		`edw_db.core.fct_authorized_transaction` - `user_id`
		`mysql_db.chime_prod.alert_authorization_events` - `user_id`
		`chime.decision_platform.real_time_auth` - `user_id`

Merchant	Merchant identification key; only populated on PIN debit Networks	`edw_db.core.fct_realtime_auth_event` - `merchant_id` `mysql_db.chime_prod.alert_authorization_events` - `merchant_id`
Network	Card network name; possible values: • `Visa` • `Allpoint` • `Discover` • `Mastercard` • `Star`	`edw_db.core.fct_realtime_auth_event` - `card_network_cd` `edw_db.core.fct_authorized_transaction` - `network_cd`

	• `Pulse`	
PAN	Displays the last 4 digits of the card number used to make the transaction as XXXXXXXXXXXX**1234**	`edw_db.core.fct_realtime_auth_event` - `pan`
PRN	Displays the Galileo Payment Reference Number (“PRN”)	This is obfuscated from display in any table for PII security.
Proc Code	Transaction type identifier (from ISO 8583; see reference table below)	`edw_db.core.fct_realtime_auth_event` - `processing_cd`

Req Amt	Transaction amount, including up-charges and acquirer fees and after any currency conversion is performed; negative amounts indicate a debit to the account, positive amounts indicate a credit to the account	`edw_db.core.fct_realtime_auth_event` - `req_amt`
		`edw_db.core.fct_authorized_transaction` - `authorization_amt`
		`mysql_db.chime_prod.alert_authorization_events` - `amount`
		`chime.decision_platform.real_time_auth` - `req_amt`

Final Amt	Transaction amount; can differ from **Req Amt** for a few reasons: • **Final Amt** includes any fees charged by Chime (like out-of-network ATM fees) • **Final Amt** will show the amount authorized if a partial authorization is performed (i.e., the Member attempts a transaction for $10, but only has $7.50 available, the $10 would be the **Req**	`edw_db.core.fct_realtime_auth_event` - `final_amt`

	Amt and the $7.50 would be the **Final Amt**) • If the Merchant performs a pre-authorization hold (like gas stations) Of note, the **Final Amt** will be the *inverse* sign of the **Req Amt** (a negative **Req Amt** will have a positive **Final Amt**, and a positive **Req Amt** will have a negative **Final Amt**) The **Final Amt** is the amount authorized/"held" from the Member's ledger balance	
Trace Number	An identifier for a transaction, generated by the message initiator (usually the merchant), that is included with all messages related to that transaction	`edw_db.core.fct_realtime_auth_event` - `trace_number`

MCC	The Merchant Category Code (MCC) is a four-digit number assigned to describe a merchant's primary business; full list can be found here	`edw_db.core.fct_realtime_auth_event` - `mcc_cd`
		
		`edw_db.core.fct_authorized_transaction` - `mcc_cd`
		
		`mysql_db.chime_prod.alert_authorization_events` - `mcc`
		
		`chime.decision_platform.real_time_auth` - `mcc`

Card Present	Indicates whether the physical card was present when the transaction was made (as indicated by the Merchant); possible values: • `YES` - Merchant indicated that the card was present during the	`edw_db.core.fct_realtime_auth_event` - `is_card_present` • NOTE: The values in the table are true/false

	transaction • `NO` - Merchant indicated that the card was NOT present during the transaction	◦ `true` = `YES` ◦ `false` = `NO`
Cardholder Present	Indicates whether the Member was physically present when the transaction was made (as indicated by the Merchant); possible values: • `YES` - Merchant indicated that the cardholder (Chime Member) was present during the transaction • `NO` - Merchant indicated that the cardholder (Chime Member) was NOT present during the transaction	`edw_db.core.fct_realtime_auth_event` - `is_cardholder_present` • NOTE: The values in the table are true/false ◦ `true` = `YES` ◦ `false` = `NO`
PIN Pad Cap	Indicates capability of Merchant terminal to accept PINs; possible values: • `0` - Unknown PIN-entry capability, or not applicable • `1` - Terminal has PIN-entry capability • `2` - Terminal has no PIN-entry capability	`edw_db.core.fct_realtime_auth_event` - `pin_pad_cap`
Acq	The identifier for the acquirer's institution	`edw_db.core.fct_realtime_auth_event` - `acq_id` `chime.decision_platform.real_time_auth` - `acq_id`
Terminal	The identifier for the terminal/device that collected the card information	`edw_db.core.fct_realtime_auth_event` - `terminal_id`

Merch	The identifier for the Merchant; assigned by the Network	`edw_db.core.fct_realtime_auth_event` - `merch_id`
		`edw_db.core.fct_authorized_transaction` - `merchant_number`
		`mysql_db.chime_prod.alert_authorization_events` - `merch_num`
		`chime.decision_platform.real_time_auth` - `merch_id`

Merch Name	The Merchant description; can include the address, state, country, etc of the Merchant	`edw_db.core.fct_realtime_auth_event` - `auth_event_merchant_name_raw`
		`edw_db.core.fct_authorized_transaction` - `merchant_name_raw`
		`mysql_db.chime_prod.alert_authorization_events` - `merch_name`
		• NOTE: the `merch_loc` field provides the address, city, state, country etc of the Merchant
		`chime.decision_platform.real_time_auth` - `merch_name`

CVV1 Result	CVV1 validation results; possible values:	`edw_db.core.fct_realtime_auth_event` -

	• `Y` — Validated • `F` — Failed • `N` or `null` — Not present	`cvv1_result`
CVV2 Result	CVV2 validation results; possible values: • `Y` — Validated • `F` — Failed • `N` or `null` — Not present	`edw_db.core.fct_realtime_auth_event` - `cvv2_result`
CVV3 Result	CVV3 validation results; possible values: • `Y` — Validated • `F` — Failed • `N` or `null` — Not present	`edw_db.core.fct_realtime_auth_event` - `cvv3_result`
AVS Result	AVS (address verification) results; possible values: • `Y` — Address and zip valid • `A` — Address only • `Z` — Zip only • `N` or `null` — None • `M` — Gift • `U` — Unsupported • `B` — AVS unused • `C` — Unrecognized AVS return value • `D` — No data • `R` — Retry AVS	`edw_db.core.fct_realtime_auth_event` - `avs_result`
AVS Info	When the transaction includes an AVS request, this field contains the data that Galileo used to calculate the AVS response	`edw_db.core.fct_realtime_auth_event` - `avs_info`

PIN Result	PIN verification results; possible values: • `Y` — Verified • `F` — Failed • `L` — Locked • `M` — PIN not set • `B` — Blocked • `N` or `null` — No PIN passed	`edw_db.core.fct_realtime_auth_event` - `pin_result_cd`
Orig Data Elems	**[TBD - unsure]**	`edw_db.core.fct_realtime_auth_event` - `orig_data_elems`
Recurring Flag	Denotes whether the merchant indicated that the card number or payment token is classified as a stored credential (which is stored by a merchant or its agent in order to process future purchases for a Member); possible values: • `YES` - Yes • `NO` - No	`edw_db.core.fct_realtime_auth_event` - `is_recurring` • NOTE: The values in the table are true/false ◦ `true` = `YES` ◦ `false` = `NO`
Cashback Amt	If cash back was requested, the amount will be populated here	`edw_db.core.fct_realtime_auth_event` - `cashback_amt`
International	Indicates whether the transaction was made internationally; possible values: • `YES` - Yes • `NO` - No	`edw_db.core.fct_realtime_auth_event` - `is_international` • NOTE: The values in the table are true/false ◦ `true` = `YES` ◦ `false` = `NO`

Trans Curr Code	The currency code for the amounts; this is the currency of the Member account and uses the 3 digit ISO 4217 numeric currency code	`edw_db.core.fct_realtime_auth_event` - `trans_curr_code`
		`edw_db.core.fct_authorized_transaction` - `currency_cd`
		`mysql_db.chime_prod.alert_authorization_events` - `cur_code`
		• NOTE: The `country_code_numeric` field in the `fivetran.csv.iso_country_codes` table contains the ISO 4217 numeric currency codes

Trans Date	Timestamp of the transaction (PST)	`edw_db.core.fct_realtime_auth_event` - `trans_ts`
		`edw_db.core.fct_authorized_transaction` - `transaction_timestamp`
		`mysql_db.chime_prod.alert_authorization_events` - `tran_timestamp`
		• NOTE: timestamp is MST
		`chime.decision_platform.real_time_auth` - `original_timestamp`

Resp Code	The response code which specifies whether a transaction is approved or	`edw_db.core.fct_realtime_auth_event` -

	denied - full list can be found here
	In some situations where the card is declined, we obfuscate this response code that is sent back to merchants, since exposing the "real" response code makes us vulnerable to card enumeration attacks (and others). When we've obfuscated the response code, this field will differ from the `original response code` field.
		`response_cd`
		`edw_db.core.fct_authorized_transaction` - `response_cd`
		`chime.decision_platform.real_time_auth` - `resp_code`

MTI	Message-type indicator (from ISO 8583; see reference table below)	`edw_db.core.fct_realtime_auth_event` - `mti_cd`
Account Status	Code indicating account status as defined by Galileo - full list can be found here or reference table below	`edw_db.core.fct_realtime_auth_event` - `account_status_cd`
Auth Code	**[TBD - unsure]**	`edw_db.core.fct_realtime_auth_event` - `auth_code`

Auth	Identifier for a transaction generated by Galileo; it's unique per subnetwork *except* for Visa subnetworks (Visa, Interlink, Plus), which all use the same counter	`edw_db.core.fct_realtime_auth_event` - `auth_id`
		`edw_db.core.fct_authorized_transaction` - `authorization_code`
		`mysql_db.chime_prod.alert_authorization_events` - `auth_id`
		`chime.decision_platform.real_time_auth` - `auth_id`

Available Funds	Available funds is the member's available balance after the auth IF the response recommended by Galileo is done. So: • For approved transactions, it's the Member's available balance after the amount of the auth has been deducted • For declined transactions, it's the Member's available balance at the time of the auth ◦ **NOTE: Auths approved by SpotMe act like declined transactions.**	`edw_db.core.fct_realtime_auth_event` - `available_funds` `mysql_db.chime_prod.alert_authorization_events` - `balance`
Card Status	Code indicating card status as defined by Galileo - full list can be found here or reference table below	`edw_db.core.fct_realtime_auth_event` - `card_status_cd`
Expiration Date	The expiration date of the card used to make the transaction	`edw_db.core.fct_realtime_auth_event` - `expiration_date`
Original Auth	The identifier in the **Auth** field of a previous transaction that is linked to this transaction • For reversals or completions, this is the identifier in the **Auth** field of the transaction that is being reversed or completed • For incremental authorizations, this is the identifier in the **Auth** field of the previous transaction in the series of transactions	`edw_db.core.fct_realtime_auth_event` - `original_auth_id` `edw_db.core.fct_authorized_transaction` - `original_auth_id`
Auth UID	Unique identifier for a transaction generated by Galileo	`edw_db.core.fct_realtime_auth_event` - `auth_uid` `chime.decision_platform.real_time_auth` -

		`auth_uid`
Is Partial Supported	Indicates whether the merchant supports partial authorizations for this transaction; possible values: • `Y` - Yes • `N` - No	`edw_db.core.fct_realtime_auth_event` - `is_partial_supported`
Risk Score	The risk score provided by the network; higher values indicate higher risk • Visa range: 0-99 • Mastercard range: 0-999	`edw_db.core.fct_realtime_auth_event` - `risk_score`
Entry Type	The method the transaction was processed; possible values: • `EMV Chip` — The card has an EMV chip that was inserted in an EMV slot • `EMV Contactless` — EMV transaction is using contactless technology • `EMV Fallback` — Unable to use the EMV chip: fallback to magnetic stripe • `Magnetic Stripe` — The magnetic stripe was read • `Contactless` — Paypass contactless transaction • `Card Not Present` — Online, mail order or telephone order • `Manual` — Manually entered information • `Other` — None of the above	`edw_db.core.fct_realtime_auth_event` - `entry_type` `chime.decision_platform.real_time_auth` - `entry_type`
Sub Network	The subnetwork name; this is the same as the **Network** field if there is no	`edw_db.core.fct_realtime_auth_event` -

	subnetwork - possible values: • `Visa` • `Visa Interlink` • `Visa PLUS` • `Mastercard Banknet` • `Mastercard Debit Switch` • `Discover` • `Allpoint` • `Star` • `Star MoneyPass` • `Star Presto` • `Pulse`	`card_sub_network_cd`
Terminal Network		`edw_db.core.fct_realtime_auth_event` - `terminal_network`
Incremental Auth		`edw_db.core.fct_realtime_auth_event` - `incremental_auth`
Original Response Code	This is the **original response code** - a field with richer meaning and more options than `response code`. Full list can be found here	`edw_db.core.fct_realtime_auth_event` - `original_response_cd`
Original Amounts		`edw_db.core.fct_realtime_auth_event` - `original_amounts`
STIP		`edw_db.core.fct_realtime_auth_event` - `stip`

EMV	For EMV transactions, this field contains a json hash of more details. For other transactions, it will just contain `{"is_emv":false}`	`edw_db.core.fct_realtime_auth_event` - `emv`
Ecommerce	For ecommerce transactions, this field contains a json hash of more details. For other transactions, it will just contain `{"is_ecommerce":null}`	`edw_db.core.fct_realtime_auth_event` - `ecommerce`
Response Code Objects	Response code objects contains a json hash of all of the response codes that apply to this transaction.	`edw_db.core.fct_realtime_auth_event` - `response_code_objects`

Processing Code Reference Table

Code	Definition
`00`	Goods/Service Purchase (with or without cash) - Debit to customer
`01`	Withdrawal/Cash Advance—Debit to customer
`02`	Debit Adjustment
`06`	Traveler's check
`10`	Money Transfer From - Debit to customer
`11`	Quasi-Cash and Scrip
`12`	Cash back from Deposit
`19`	Consumer Fee Collection
`20`	Return (of goods) - Credit to customer
`21`	Deposits/Deposit Payments
`22`	Credit Adjustment

`24`	Check Deposit/Payment To without an Envelope
`25`	Cash Deposit/Payment To without an Envelope
`26`	Money Transfer To - Credit to customer
`28`	Prepaid card load/activation
`29`	Consumer Funds Disbursement
`30`	Available funds inquiry (generally used for an inquiry for the amount available for a POS transaction)
`31`	Balance inquiry (generally used for ATM balance inquiries)
`33`	Account Verification Inquiry
`39`	Generic Account Balance Inquiry
`40`	Cardholder Account Transfer
`50`	Payment (3rd-party payment transaction, payee-initiated)
`55`	Payment Receipt (3rd-party payment transaction, payer-initiated)
`58`	Transfer Payment (Intra-financial institution payment transaction)
`59`	Payment enclosed
`72`	Prepaid card activation
`90`	PIN change
`91`	Information inquiry
`92`	Notification to bank

MTI Reference Table

See [MTI Codes Decoded]

Code	Meaning	Usage

`0100`	Authorization Request	Dual message system (DMS); determines if funds are available to get an approval, but does not post to the Member's account for reconciliation.
`0110`	Authorization Request Response	Request response to a point-of-sale terminal for authorization for a cardholder purchase.
`0120`	Authorization Advice	When the point-of-sale device breaks down and you have to sign a voucher.
`0130`	Authorization Advice Response	Confirmation of receipt of authorization advice.
`0200`	Financial Transaction Request	Single message system (SMS); determines if funds are available to get an approval AND posts directly to the Member's account for reconciliation.
`0210`	Financial Transaction Request Response	Issuer response to request for funds.
`0220`	Financial Transaction Advice	Advice that a reconciliation action has taken place (aka, a settlement within the DMS); receiver can only accept, not reject.
`0230`	Financial Transaction Advice Response	Issuer confirmation of receipt of financial advice.
`0400`	Acquirer Reversal Request	Reverses the action of a previous transaction.
`0410`	Acquirer Reversal Request Response	Issuer response to reversal request.
`0420`	Acquirer Reversal Advice	Advises that a reversal has taken place.

Account Status Reference Table

Status	Description
`C`	Canceled
`D`	Disabled

`F`	Failed ID verification
`J`	Suspended/never activated
`K`	Suspended
`M`	Moved to new program; i.e., the cardholder has been migrated to a new program - this status is functionally identical to status: `Z`
`N`	Active
`P`	Passed ID verification
`Q`	Delinquent
`R`	Charged off
`T`	ID verification in process
`U`	Upgraded
`V`	Application submitted; the account setup process has not completed - the exact steps in the setup process vary according to the ACSET product parameter
`W`	Waiting to be processed
`Z`	Canceled without refund
`c`	Canceled, awaiting repayment

Card Status Reference Table

Status	Description
`A`	Lost card waiting for sufficient funds
`B`	Blocked This may be an un-issued instant issue card that is used at a point of sale before the card has been sold, or the card reached the maximum number of PIN retries
`C`	Canceled

`D`	Disabled This may indicate that a card has been reissued or replaced and the bounce-mail flag is set to Yes
`L`	Lost Card If reported lost with Modify Status type 3, a replacement card is issued with a new PAN - see the Lost, Stolen, or Damaged Cards guide for more information
`N`	Active (normal) A card and its account **must be in this status for a card transaction to be successfully authorized** • **The exception is an advice or force post, which must be accepted regardless of account status**
`O`	Operations Hold This may indicate that the embosser has run out of plastic to emboss cards
`Q`	Delinquent
`R`	Charged Off
`S`	Stolen Card If reported stolen with Modify Status 4, a replacement card is issued with a new PAN - see the Lost, Stolen, or Damaged Cards guide for more information
`V`	Voided
`W`	Waiting for Payment **This is the default status of a newly created card**, or a replacement card that does not have sufficient funds to cover a replacement fee
`X`	Set to Emboss The card will be picked up by an automated process and sent to the embosser
`Y`	Shipped/Ready to Activate The card order has been sent to the embosser
`Z`	Canceled without Refund