EMV Comes to the Virtual Terminal

80145507-001

Rev. A

11/11/2016

http://www.idtechproducts.com
10721 Walker Street, Cypress, CA 90630, USA Voice: (714) 761-6368 Fax: (714) 761-8880

Revision	Date	Description	By
01	08/30/2016	Initial Draft.	Randy P
A	11/11/2016	White paper version.	Kas T

http://www.idtechproducts.com
10721 Walker Street, Cypress, CA 90630, USA Voice: (714) 761-6368 Fax: (714) 761-8880

Executive Summary

EMV adoption has proven challenging for merchants (especially small to midsize businesses), and in the U.S., many consumers have found chip-card transactions to be slow and inconvenient. Quick Chip technology (pioneered by Visa, but embraced, also, by other leading card brands) brings EMV transaction times down to around two seconds, but until now, virtual terminals have not been able to leverage this technology, for technical reasons. ID TECH's patent-pending Augusta card reader brings together Quick Chip technology, USB keyboard mode, and a proven EMV L2 kernel for the first time. The result is an EMV solution that makes it exceptionally easy for virtual terminal customers to benefit from two-second transaction times while minimizing PCI-DSS scope.

Virtual Terminals: EMV-Ready?

Traditionally, “card present” payment processing has been accomplished through the use of magnetic-stripe card data captured via a magstripe card reader (MSR), with the card and payment data sent (in real time) to a payment gateway/processor for authorization. This "swipe and go" technology is often physically realized in terms of a dedicated card reader connected to a phone line or internet connection, but it is also often achieved using so-called *virtual terminal* technology, wherein a PC, laptop, or tablet offers a web interface to an online application that accepts card data. Typically, the application's data fields are populated automatically by the output of a card reader operating in "keyboard mode," connected to the PC via the Universal Serial Bus. When a merchant (or customer) swipes a card through the reader, track data appears in the application; that data, along with the transaction amount, is then sent to the authorizing party (via a gateway) with the click of a button.

Such a scenario becomes challenging when a chip card enters the picture. No conventional contact-EMV card reader operates in "keyboard mode." Even if it did, the various card-to-reader and reader-to-application communications that happen in an EMV transaction must be carefully choreographed by the application software, and the software must be ready to handle any number of scenarios in which the chip card, the reader, or the application itself might encounter an error, or decline the transaction, either before *or* after going online for authorization. In addition, the application needs to process a variety of kinds of EMV-associated data, beyond mere "track data." Because of the comparatively complex communication and data-processing requirements of the typical EMV application, integration of EMV readers into the virtual-terminal scenario tends to be challenging; and doing it in a way that reduces merchant PCI scope is both time-consuming and expensive.

Quick Chip: EMV That's Not Just Fast, But Simple

Quick Chip technology, introduced by Visa early in 2016 (now accepted by all major card brands), was originally proposed as a way to make EMV transactions *faster*. It succeeds in doing this, by making EMV *simpler*.

Conventional EMV distributes the logic of transaction approval between the card (which contains a chip), the reader (which contains an EMV kernel), the application, and the issuer, or online authority. The number of possible approval-decision scenarios is correspondingly large. In most cases, the chip card (ICC) is consulted at least twice before a transaction is officially considered approved or declined. When the chip is presented with a decision request, the response (assuming nothing *requires* the transaction to be aborted) is usually advice to the effect "go online." The application then requests approval from an online authority. But the advice from the online authority is not binding. In fact, in a conventional EMV transaction, the chip is consulted a second time, and the card is entitled to decide (on the second consultation) whether to override the online approver's decision. Note that all of these consultations and decisions need to happen while the card remains inserted in the reader. Hence, it is not unusual for a chip card transaction to take ten seconds or more.

Visa realized that the "card inserted" time could be shortened dramatically if the card were to be consulted only once, with the cardholder free to remove his or her card from the machine immediately after data is read. Quick Chip implements exactly this scenario. In a Quick Chip transaction, the chip card advises the application to go online within roughly two seconds of card presentation, and the customer is free to remove his/her card immediately, at that point. The application typically goes online with an approval request while the customer is putting his or her card away. When the online decision comes, that decision is then binding, and a receipt can be printed.

From the cardholder's standpoint, Quick Chip simply provides a "dip-and-go" alternative to the usual swipe-and-go MSR interaction. Either kind of transaction takes the same amount of time. Each one immediately returns "transaction data" to the application — data that can be used for obtaining online authorization (and for printing a receipt).

Keyboard Mode: Essential for Virtual Terminals

Because of the elaborate back-and-forth communication requirements of traditional EMV, most chip card readers use USB in so-called HID mode, rather than in Keyboard mode. This is an important distinction, because a USB-HID device requires dedicated driver software to enable communication with the host, whereas a USB-Keyboard device requires no special drivers; you simply plug it in, and it works.

The use of USB in HID mode is problematic not just because special drivers (with host-specific installation requirements) are needed, but because browser- or web-based virtual terminal software cannot connect to a USB port directly, in any case; the browser is not USB-aware, and applications written in HTML cannot connect to a device on a serial port. Hence, there is no easy way to get data from a USB-HID device to show up in a browser window or web form, regardless of which drivers are installed.

By contrast, card readers that operate in USB Keyboard mode can send data (as "keystrokes") directly to a web form. This makes it easy to connect USB-KB card readers to virtual terminal apps. But unfortunately, such readers tend to be MSR-only. *Until now*.

ID TECH Augusta with Quick Chip

The patent-pending Augusta-series card reader from ID TECH incorporates magstripe as well as EMV capability, with Quick Chip as an option. When Quick Chip is enabled, chip-card interactions take place in USB Keyboard mode, with no need to install special drivers. Inserting a chip card into the reader results in data streaming directly into the payment app. Keystroke data will show up at the insertion point of the cursor, the same as with any USB-KB magstripe reader.

As with other readers, the Augusta can be set up to output encrypted data, or unencrypted data. This means that if the virtual terminal application is appropriately certified, and the Augusta is key-injected, with encryption enabled, the merchant can operate with a significantly reduced PCI DSS scope, while enjoying the liability-protection benefits of EMV.

ID TECH is the only vendor to offer a fully EMV-compliant card reader that can operate in USB Keyboard mode (while also offering fallback-to-MSR capability, again in Keyboard mode), with two-second transaction times, with or without AES or TDES encryption. As with other ID TECH products, the Augusta (available in SRED and standard configurations) uses ID TECH's proven EMV L2 common kernel.

Quick Chip Mini-FAQ

Is it really EMV?
Yes. Quick Chip is compliant with EMV and is an EMV modality accepted by all major card issuers. The underlying implementation relies on ID TECH's well-proven EMV L2 common kernel, used in all of ID TECH's EMV products.

For what market is Quick Chip intended?
Quick Chip is an online-only technology, which makes it ideal for the U.S. market (which is a predominantly online market), although it can also be used in other geographies and settings.

Does Augusta with Quick Chip support fallback to MSR?
Yes. Augusta offers conventional magstripe capability as well as contact EMV capability. Magstripe data (encrypted or unencrypted) is available in Keyboard mode, like Quick Chip EMV data. Hence, the unit is fallback-capable.

Is Augusta with Quick Chip available in an SRED model?
Yes. The SRED model is PCI 4.x-approved and supports tamper protection, MAC protection of commands, and fulltime encryption, among other high-end features.

Does the standard Augusta model provide encryption?
Yes. The standard unit supports DUKPT key management and data encryption using AES or TDES. Also note: ID TECH is a TG3-certified key injection facility.

How It Works

In Quick Chip mode, ID TECH's Augusta is preconfigured to detect the insertion of a chip card in the ICC slot and carry out all of the steps of a Quick Chip EMV transaction, up to (but not including) going online for authorization. The steps include the following:

1. If the card is inserted correctly, the reader's activity light will change from blue to green. (If not, it will change to red.)
2. Firmware kicks off the EMV transaction with an arbitrary initial transaction amount (configurable) that's higher than the Floor Limit, to force the card to give "go online" advice.
3. Augusta's EMV kernel executes all necessary steps of the EMV transaction, updating Terminal Verification Result flags as necessary, then sends a Gen AC request to the card.
4. When a card decision is reached and an ARQC is generated by the card in conjunction with advice of "go online," Augusta firmware requests transaction data for all the tags that were specified in the terminal configuration settings. (A proprietary tag is used to specify which TLVs are returned in this step.)
5. The requested TLVs are collected and then output as ASCII-Hex ("character") data over the USB-KB interface.
6. Augusta's ICC-slot-light begins to flash, and the unit beeps audibly, unit until the card is removed from the ICC slot. (When the card is finally removed, the slot-light stops flashing, and the green activity-indicator light returns to blue.)
7. Firmware, meanwhile, continues the transaction with an ARC (result code) of 'Z3' – Unable to Contact Host – in tag 8A. (This is the second Gen AC.)
8. The card, upon learning of the Z3 result, issues an AAC. Normally, this cryptogram indicates a Declined transaction. But in this case, the card's decision is not the final decision.

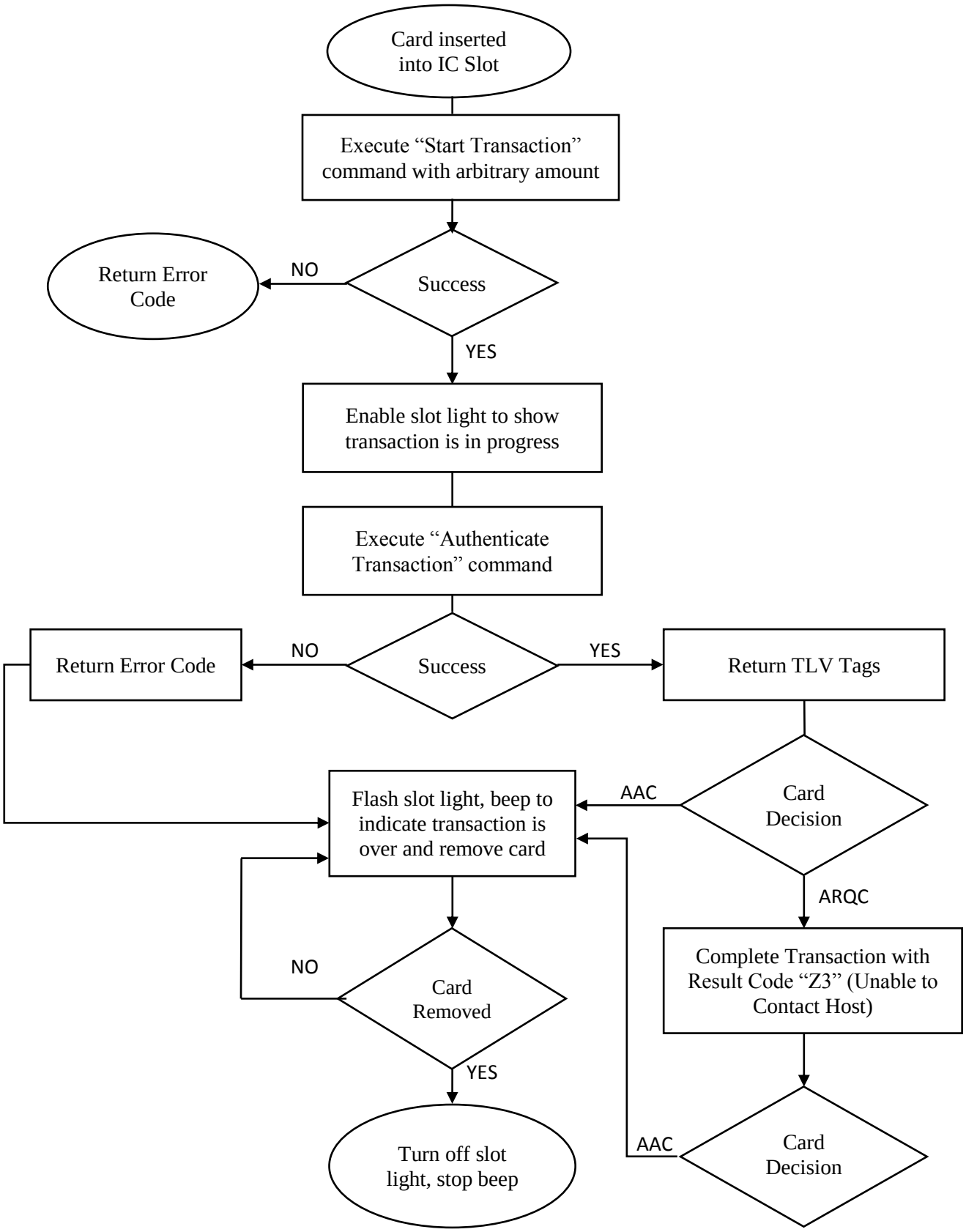
The terminal application will send the TLV data from Augusta (plus any other required fields, like Final Amount) to the gateway, which will (in turn) use the appropriate data object list to go to the authorizing party for approval. When the online authorization decision is relayed back to the virtual terminal, that decision is the final decision, and any necessary customer receipts can be printed at that time.

Note that because the transaction sequence can be initiated without the Final Amount yet known (it's provided, by the terminal, at the *end* of the sequence), the card doesn't have to sit in the machine while the Final Amount is being tallied. Thus, card-inserted time is reduced.

These steps reflect standard Visa Quick Chip Specification choreography. All are within EMV guidelines and meet card issuer requirements for EMV.

A conventional EMV transaction includes additional steps (after the second Gen AC) involving Issuer Authentication and (optionally) issuer scripts. These steps are not possible in Quick Chip, since the card is no longer present.

Note: A flow diagram, showing Quick Chip program flow, is presented on the next page.



What the Data Looks Like

In Quick Chip mode, ID TECH's patent-pending Augusta outputs a single character stream that consists entirely of TLV data. The data can (and will) vary in composition depending on configuration-time choices, but data typically looks as follows:

```
DF EE 25 02 00 02 DF EE 26 02 20 00 DF EE 12 0A 62 99 49 00 75 00 02 A0 02
92 DF EF 5D 11 47 61 CC CC CC CC 04 32 D1 01 22 01 CC CC CC CC CC 5718 5F
3D 1D AD 0C 82 FB C9 C1 C1 0A 22 C8 B8 5E 1C 32 76 20 22 36 77 CF F8 DF EF
5B 08 47 61 CC CC CC CC 04 32 5A 08 5F 3D 1D AD 0C 82 FB C9 5F 20 1A 56 49
53 41 20 41 43 51 55 49 52 45 52 20 54 45 53 54 20 43 41 52 44 20 34 33 5F
24 03 10 12 31 5F 25 03 95 07 01 5F 28 02 08 40 5F 2A 0208 40 5F 2D 00 5F
34 00 5F 57 01 00 50 0B 56 49 53 41 20 43 52 45 44 49 54 4F 00 82 02 5C
00 84 07 A0 00 00 00 03 10 10 8C 15 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A
02 9A 03 9C 01 9F 37 04 8D 17 8A 02 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A
02 9A 03 9C 01 9F 37 04 8E 0E 00 00 00 00 00 00 00 00 1E 03 02 03 1F
00 9C 01 00 9F 02 06 00 00 00 00 00 00 9F 03 06 00 00 00 00 00 00 9F 10 07 06
01 0A 03 21 99 00 9F 13 00 9F 20 00 9F 26 087D 13 81 E6 41 67 31 0B 9F
27 01 00 9F 34 03 1E 03 00 9F 36 02 01 06 9F 37 04 14 41 90 19 9F 38 00 9F
39 01 07 9F 4D 00 9F 4F 00 95 05 42 C0 00 00 00 9B 02 E8 00 8A 02 5A
33 99 00 9F 5B 00
```

Here, all TLV tags are shown in blue; lengths are in orange; data values are brown. Spaces have been inserted between byte values for clarity. (In normal operation, Augusta outputs a continuous stream of characters.)

Some tags are ID TECH (proprietary) tags. For example, the transaction KSN is contained in the DFEE12 tag.

Normally, this entire block of data will be sent by the virtual-terminal app to a gateway that can process it further. But note that the above data can (optionally) be intercepted in real time by means of standard *keydown* or *keypress* event handlers attached to a web-page DOM element. Thus, pre-processing can optionally occur on the client, using JavaScript.

A live demo app (implemented as a web page) is available at http://idtech.ws/qc/, showing key-handler-based processing of tag data in JavaScript. (Of course, to see the app in actual operation, you'll need to plug an Augusta into your laptop or tablet.)

Conclusion

ID TECH's patent-pending Augusta with Quick Chip offers the industry's only Keyboard-mode-enabled EMV solution suitable for virtual terminal use. For the merchant, it offers an easy way to accept chip card transactions (and enjoy the liability-protection benefits of EMV) while minimizing PCI-DSS scope. As a bonus, the merchant is able to offer customers unparalleled speed and ease of use, with EMV transaction times of only two seconds (greatly reducing the chance that a customer will accidentally leave a card behind, in the reader). Since the Augusta is a USB Keyboard device, there are no special drivers to install; an EMV virtual terminal can be entirely web-based. Merchants and customers enjoy all the speed and convenience of MSR transactions, with the security and liability protection of EMV.