



EMV Best Practices and Business Requirements for ATM Deployment

About Debit Network Alliance

Debit Network Alliance LLC (DNA) is a Delaware limited liability company owned by 10 U.S. Debit Networks, and open to all U.S. Debit Networks, founded in December 2013. The goal of this collaborative effort is to provide interoperable adoption of chip technology for debit payments, while supporting security, innovation, and optimal technology choice. Further the company has worked to bring about perpetual access to the technology deployed to accomplish EMV in the US, and support for all transactions types (PIN, signature, no-CVM) supported by the debit networks both existing and future.

The debit networks have a long history of working collaboratively - especially with regard to improving security - to define standards that maintain the integrity and quality of the U.S. payment industry.

The founding networks of Debit Network Alliance are AFFN[®], ATH[®], CO-OP Financial Services[®], Jeanie[®], NETS[®], NYCE[®], Presto![®], PULSE[®], SHAZAM[®], and STAR[®].

U.S. Deployment

The global brands have announced roadmaps with liability shift incentives, but deployment on debit has been stalled due to the complexity inherent in debit in the US. Credit cards are much simpler than debit because there is only one brand per card. On the debit side, there are multiple US debit networks on a card and Durbin network requirements specifically for debit. These requirements and recent court rulings uphold merchant routing choice and a need to “future proof” functionality in case of further regulatory action.

Furthermore, issuers want to maintain their ability to easily switch networks for business reasons without reissuing cards.

How It Works At an ATM

EMV at the ATM is the capability to support and process EMV chip cards at ATMs using an EMV chip card reader. EMV transactions at ATMs are processed with Online PIN – the encrypted PIN is verified online by the issuer/host.

When a cardholder inserts his or her card, it initiates a secure interface with the device. The ATM establishes that the card has a chip and selects a matching application. It will then read all the data from the card perform checking, verification and risk management. The application determines and enforces the rules of payment stored on the card. Next, the application generates a cryptogram value and subsequently sends this data to the host.

The host switch application is responsible for managing chip data and scripts which include the application cryptogram and cryptogram information data, issuer application data, application transaction, transaction date, type and amount.

The host also performs all the usual transaction authorization checking including getting authorization from the issuer. The host then performs the authorization, decrypts PIN block and validates against specific cardholder. The cryptogram is verified to confirm that the chip is not counterfeit. A return cryptogram is generated and sent back to the chip in the authorization response.

Once these steps are complete, the data is sent back to the ATM. The ATM performs an external authentication to check that the host is valid and validates the response cryptogram. It accepts final authorization to decline or approve and the transaction is completed. The final step is to update the integrated circuit card with script data received by the host.

Applications and AIDs

The application is the payment software installed on the chip that runs the EMV authentication process. It contains the parameters that are used during the interaction between the card and the terminal.

AIDs tell the EMV Reader (POS device or ATM) which applications and networks are available for authorization. It is written onto the chip during card production and identifies the owner of the application and also things like the cardholder verification methods available for that card.

There can be multiple AIDs on a card. However if there is only one proprietary AID on the card, the transaction routes to the owner of that AID. For example when the Global MasterCard AID is selected, the transaction must be sent to MasterCard, just as when the Global Visa AID is selected the transaction must be sent to Visa. There are two issues with only one proprietary AID on the card ; one, it does not comply with Regulation II regarding POS routing choice and; two, it does not comply with debit network priority routing rules which define in the BIN file which network the issuer contracted priority routing with for ATMs.

If there are multiple AIDs on the card, the terminal must be able to prioritize which AID to select according to the acquirer choice, not according to standard EMV priority logic. This again suggests picking the US Common Debit AID as the only way to support debit network priority routing rules and the BIN file flag for ATM priority routing.

EMV Debit AIDs

For purposes of this document, Global Brand AID means the AID present on the card that is utilized by the global brand whose logo is on the card. Global AIDs include VISA, MasterCard, Discover, American Express, etc.

The U.S. Common AID means the AID present on the card that is owned by one of the global brands, but licensed by multiple debit networks. Any debit network licensed on a U.S. Common AID is available through this AID.

Why This Is So Important To Know

Terminals today only support priority selection of the Global AIDs. ATM owners (or merchants) do not want the issuer or cardholder to make the routing decision. They want to continue to route using

current routing methodology. So, if there is a US Common AID on the card, the terminal needs to allow it to be selected over the Global AID when the card and terminal support both.

Ability for the terminal to prioritize AID selection is important to maintain routing choice. Network availability is through the use of the Common AID. Deploying ATMs without this new US logic will mean that all transactions at those ATMs will be routed to the global brands only.

Why the U.S. Common AID

The Common AID provides choice similar to the magstripe for any debit network which has licensed the Common AID on that card. Only one Common AID will be present on a Card. For example, if it is a Visa branded debit card, the card will have the Global Visa AID and the Visa US Common AID. It would not have the Maestro US Common AID. Any debit network which licenses the Common AID on that card would be available for routing. This allows you to maintain existing relationships with surcharge free networks etc., and provides the maximum flexibility in creating and managing the profitability of your acquiring programs.

Business Requirements for Terminal Changes to Enable AID Selection

Development may need to be done by the terminal manufacturer to allow the terminal to select the AID the acquirer wants, rather than operating with the standard EMV logic. This may potentially be done by the acquirer processor if it can be coded in the load versus the ATM software. Below are the recommended business requirements needed in order to achieve this.

- The terminal must be able to recognize if there is a Common AID present on the card.
- If one is present, the terminal must be able to override standard EMV priority selection of the AID.
- Terminal should have logic that allows the acquirer to either select the Common AID through configurable parameters, or select the Common AID as the default. It is expected that the second option will be the easiest for most terminal manufacturers.
- If the Common AID is not present, the terminal should use standard EMV logic of AID and application selection.
- Software changes should not be done in the EMV kernel itself in order to prevent recertification by EMVco.

ATM Deployers' Checklist

1. Load the Global and Common AIDs
2. Check with each network for a list of AIDs which may be supported on the cards
3. Understand how the terminal manufacturers plan to support AID prioritization and selection
4. Verify and test terminal for AID prioritization and selection
5. Keep in mind that Networks' Operating Rules may vary