SMART PAYMENT ASSOCIATION

Strengthening Card Authentication: a migration to DDA

An SPA White Paper

First issued in October 2009 – Updated July 2015

July 2015

Table of Contents

1. Introduction

In the fight to combat card fraud, a key objective is to make the data - which the fraudsters want to get their hands on – useless. This can be accomplished by making each transaction unique. There is no value in stealing account numbers and expiry dates if these are accompanied by a unique set of data that can only be verified by a trusted party.

In face-to-face transactions, public and private key cryptography are employed to achieve this goal. The success of these methods has driven the worldwide introduction of smart (chip) payment cards, and of course, the adoption of the EMV standard (www.emvco.com).

Initially, Card Authentication Methods (CAMs) were based on Static Data Authentication (SDA). However, the world has moved on, and the vast majority of payment cards shipped today feature the more sophisticated Dynamic Data Authentication (DDA) or Combined Data Authentication (CDA).

For those banks and regions that continue to use the SDA method, it's time to change. As we'll explore in this paper, the opportunities to be gained from a migration to DDA are significant – not least in improved security, the associated reduction in fraud, and the enablement of the "finer" control of offline transaction approvals.

First published in 2009, this SPA paper has been updated in 2015 to reflect the evolving technology and commercial environment - to provide an overview of the CAM marketplace, the role of SDA and the increasing adoption of DDA and CDA schemes.

1.1. EMV CAM Methods

Let's first take a look at the key differences between legacy SDA and today's more modern authentication methods.

In SDA, merchant terminals verify digital signatures stored in cards against the public key certificates stored in the terminals. With SDA, the digital signature used to authenticate the card is identical for each transaction – indeed it is stored in the card on the day the card is personalized for the end-user. Hence, it is possible (although difficult) to reproduce the digital signature of an SDA chip card because the same authentication data is always used for all offline transactions; consequently, a merchant terminal working offline would believe such a card to be genuine. It should be noted that reproducing a chip card in this manner requires sophisticated skills and any such attempt would fail should the transaction be sent online to the issuer.

With DDA and CDA, however, the offline authentication data is unique to each transaction. The card responds to a random challenge from the terminal. This means that even if the data is successfully copied, the counterfeit card would fail to be authenticated. Cards must have a cryptographic coprocessor to support DDA and CDA, and are therefore more complex than cards that only support SDA.

Issuers should also note that Personal Identification Number (PIN) verification is done in clear text for SDA, while it can be encrypted with cards supporting DDA. This is in line with PCI best practice to never allow the PIN to be presented in clear text.

So while SDA cards offer a higher level of security compared to magnetic stripe cards, and have been very efficient in combating fraud worldwide, they still leave a narrow window of opportunity for crime: firstly by presenting static data within transactions and secondly by allowing the PIN to pass in clear text between PIN pad and card.

This is a major concern that is preventing the widespread usage of EMV cards in offline applications (source: VISA Mandate).

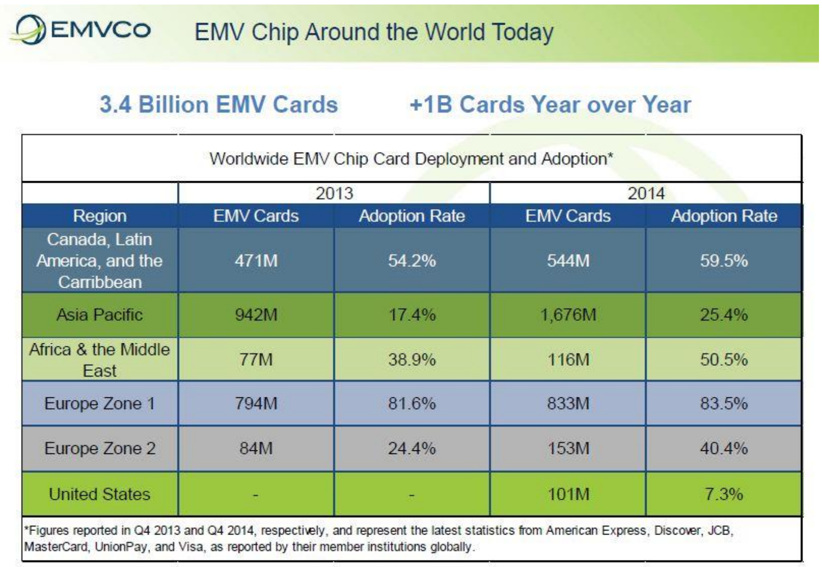
1.2. Benefits of EMV

There is no doubt that the widespread adoption of the EMV standard has dramatically reduced fraud where it has been deployed. In Europe, for example, counterfeit card fraud losses continue to decrease because EMV has made it much harder for criminals to use fake cards in cash machines and shops.

Taking the European Central Bank’s figures, the card fraud-related share in the value of transactions fell from 4.5 basis points in 2007 to 3.8 basis points in 2012, its second lowest level since 2007.

Today over 80% of the payment cards and 99% of terminals in Europe* are EMV-based (source: EMVCo).

Figure 1: Worldwide EMV adoption (source:EMVCo)



EMVCo EMV Chip Around the World Today

3.4 Billion EMV Cards +1B Cards Year over Year

Worldwide EMV Chip Card Deployment and Adoption*

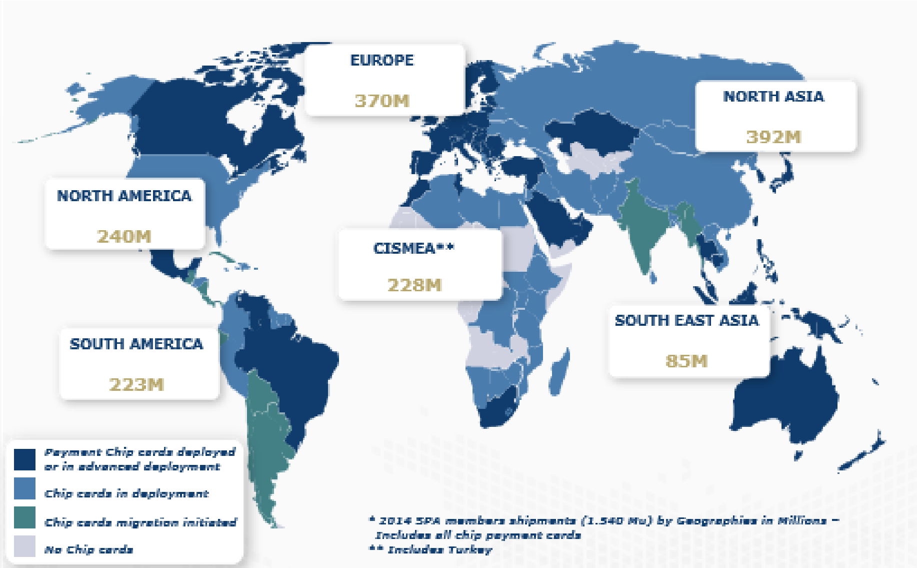
	2013		2014	
Region	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate
Canada, Latin America, and the Carribbean	471M	54.2%	544M	59.5%
Asia Pacific	942M	17.4%	1,676M	25.4%
Africa & the Middle East	77M	38.9%	116M	50.5%
Europe Zone 1	794M	81.6%	833M	83.5%
Europe Zone 2	84M	24.4%	153M	40.4%
United States	-	-	101M	7.3%

*Figures reported in Q4 2013 and Q4 2014, respectively, and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member institutions globally.

In the US, the card fraud-related share in the value of transactions is 10.4 basis points, and 8.7 basis points in Canada. This clearly demonstrates that card fraud losses are higher in countries where EMV migration is not complete (Canada) or has just started (US) (source: Payments Card, and Mobile and Alaric Fraud Report 2015).

1.3. The Move to DDA

With deployments taking off in all regions of the world, EMV is becoming a truly established, global and interoperable infrastructure. China Union Pay has by and large converted all cards to chip, meanwhile the US is the largest territory in which migration is currently well underway. Both markets have, by large, chosen to use DDA.



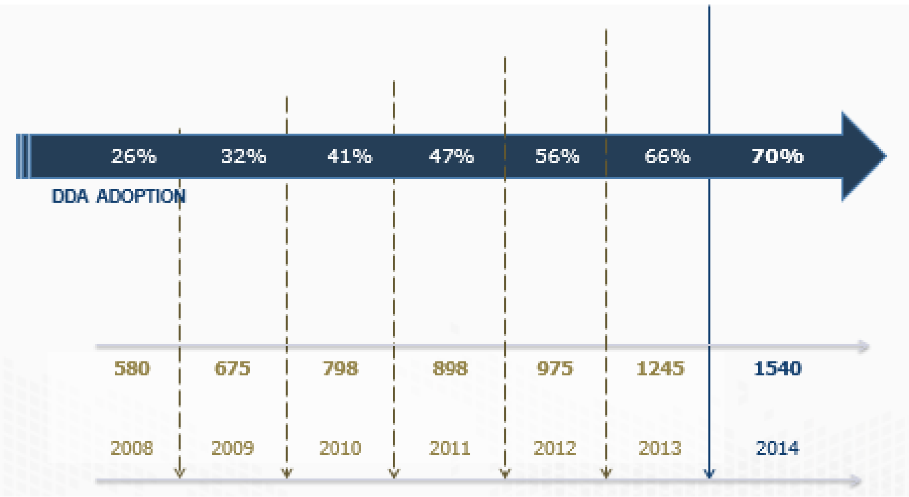
* 2014 SPA members shipments (1.540 Mu) by Geographies in Millions – Includes all chip payment cards
** Includes Turkey

Figure 2: SPA 2014 EMV shipments (source: SPA)

With DDA representing 70% of SPA shipments globally - with a 30% growth in 2014, it can therefore be accurately stated that, due to its effectiveness in combating counterfeit fraud, dynamic authentication is growing in popularity to become the de facto standard for card schemes and issuers around the world.

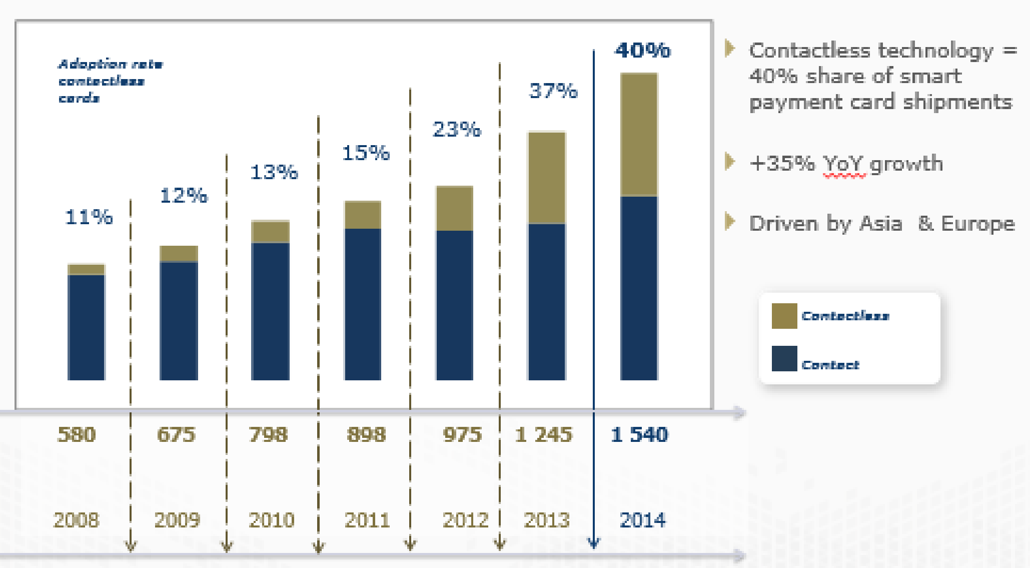
But dynamic authentication is just part of the story. The mass take-up of innovative new payment propositions by consumers is fuelling a huge growth in demand for contactless technologies - with over 600 million contactless cards delivered by SPA members in 2014.

Figure 3: DDA represents 70% of SPA shipments in 2014 (source: SPA)



So, while the priority for issuers might be improving the inherent security of their cards, this doesn't add much in the way of end customer value proposition. For this reason issuers should consider going contactless when starting their deployment of dynamic authentication – enabling them to surprise and delight consumers with greater speed and convenience, while also closing the door to criminals.

Figure 4: Contactless represents 40% of SPA shipments in 2014 (source: SPA)



- Contactless technology = 40% share of smart payment card shipments
- +35% YoY growth
- Driven by Asia & Europe

2. DDA Helps Fraud Reduction – but “Why?” and “How?

Adoption rates of DDA on EMV cards have increased as major payment schemes push forward rules and recommendations endorsing DDA due to its best-in-class security and functionality relating to payments at physical point-of-sale.

In Europe, EMV technology has become standard for chip payment cards. In comparison to magnetic stripe cards, EMV cards based on Chip and PIN continue to be deployed, offering higher security level during transactions.

When the threat of copying the magnetic stripe details was first identified, Chip and PIN made it harder for criminals to create a fake card. As already shown, counterfeit card fraud losses are continuing to decrease in Europe, thanks to EMV, which has made it much harder for criminals to use fake cards in cash machines and shops in Europe.

As EMV migration approached completion in the continent, both VISA and MasterCard decided to publish plans for phasing out SDA – making transactions unique.

2.1. The Benefits of DDA

DDA’s dynamic authentication process provides unique data for each transaction together with elevated PIN protection. Together these make DDA chip cards equipped with a crypto-processor the most appropriate solution to prevent counterfeit fraud losses in this particular domain.

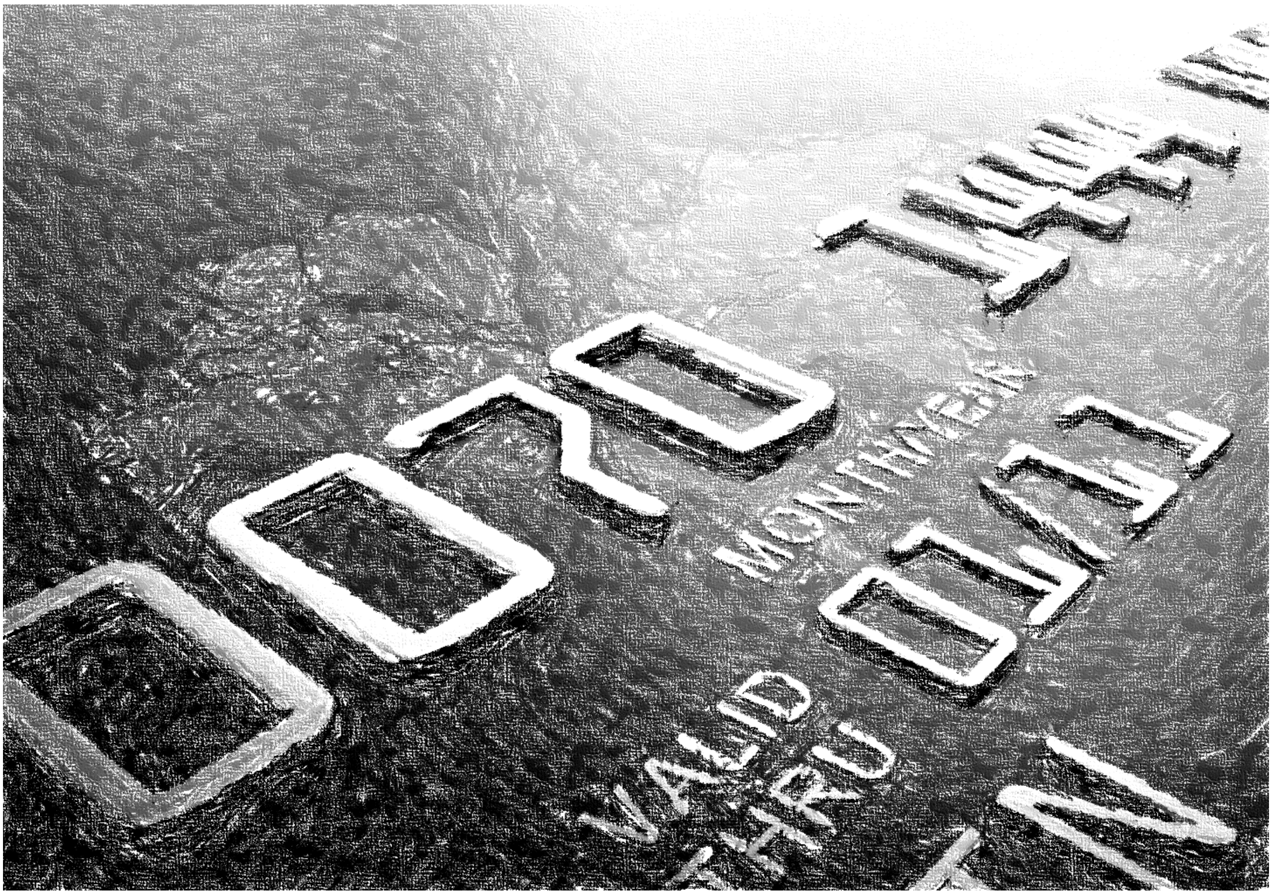
Dynamic Data Authentication caters for the following business interests:

- enables the ability to always present the PIN as encrypted
- provides the opportunity to increase transaction footprint. DDA is an appropriate solution for offline transactions; low value payments, contactless payment, or pre-authorized payment transactions such as transport or vending machines
- reduces transaction cost. Highly secure offline authentication is a great advantage when the communication costs are high or in countries with a poor communication infrastructure
- delivers a consistent user experience (for both off and online transactions)
- avoids losing transactions at offline locations.

The migration to DDA with contact cards has also helped facilitate the migration to a contactless payment ecosystem, as banks have decided to embrace contactless together with the higher security standard of DDA.

Countries with high EMV maturity levels have typically followed a natural migration path: SDA, DDA, Dual Interface (a card with a single chip that features both a contact and contactless interface).

Regions and countries that have migrated to EMV more recently, however, have moved directly to the level mature countries have reached – in other words, DDA Dual-Interface EMV Chip and PIN cards. In many ways this is comparable to how some countries that didn't employ check books went directly from cash to card. In China, for example, the EMV program jumped directly to a DDA Dual Interface from the get go.



3. VISA and MasterCard Mandates

Both VISA and MasterCard have issued new mandates relating to their respective CAM (Card Authentication Method) offline policies which will come into effect gradually, starting in 2015.

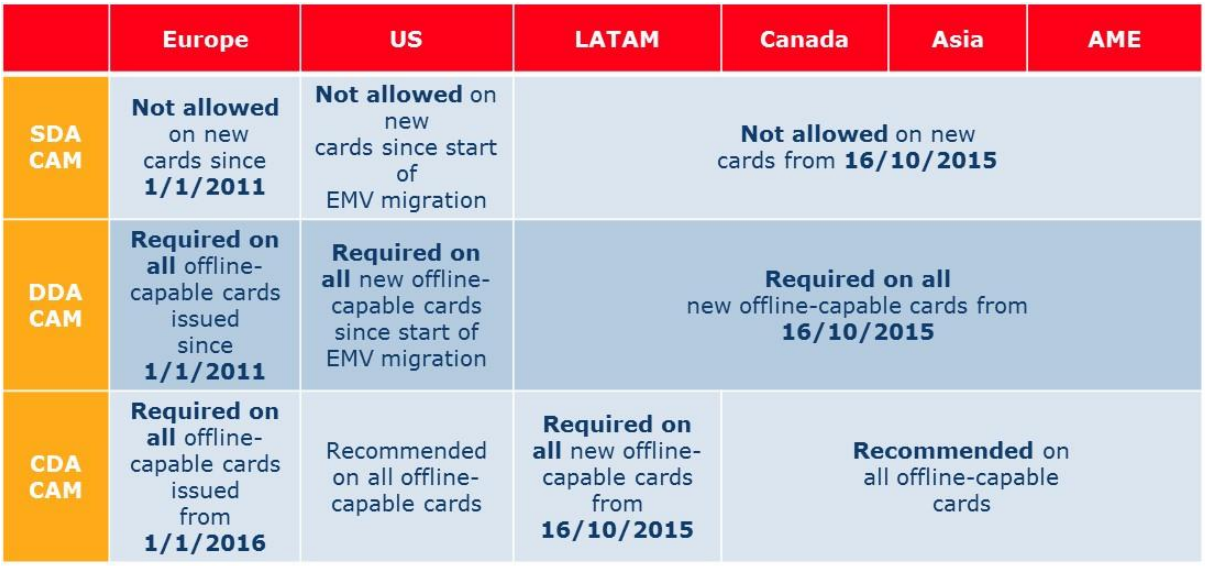
- "ONLINE only" cards
  - The transaction is systematically authorized on the Issuer host: card does not allow transactions offline
  - Any chip products can be used (SDA/DDA/Dual Interface)
  - VISA and MasterCard will allow Online Only cards worldwide.

- "OFFLINE capable" cards
  - The card can be authenticated by the POS and following a successful verification, transactions can be approved offline
  - The card must support at least one offline CAM method listed in Figure 8.

3.1. MasterCard's Mandate Principles

- SDA CAM Offline is to be removed in all markets
- DDA mandated on all Offline programs
- Online-only products are allowed in all regions for all brands in contact (in an online-only product, no SDA certificate is added in the card but issuers verify that a card is genuine based on data in the authorization requests based on a Triple DES algorithm).

Figure 6: MasterCard mandate overview by geography

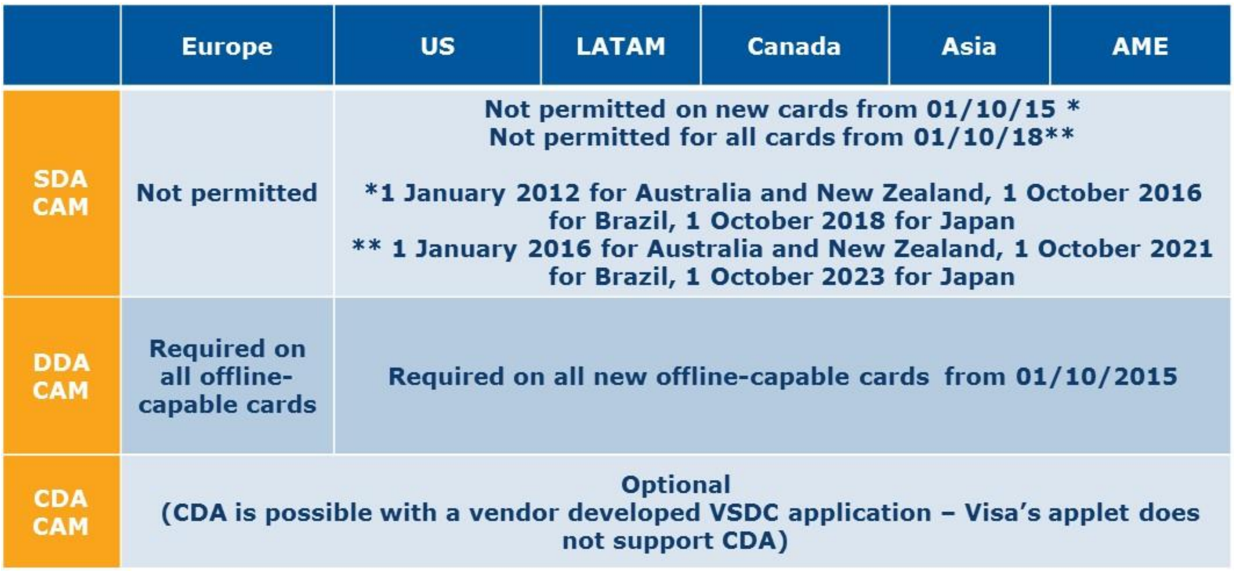


	Europe	US	LATAM	Canada	Asia	AME
SDA CAM	**Not allowed** on new cards since **1/1/2011**	**Not allowed** on new cards since start of EMV migration	**Not allowed** on new cards from **16/10/2015**			
DDA CAM	**Required on all** offline-capable cards issued since **1/1/2011**	**Required on all** new offline-capable cards since start of EMV migration	**Required on all** new offline-capable cards from **16/10/2015**			
CDA CAM	**Required on all** offline-capable cards issued from **1/1/2016**	Recommended on all offline-capable cards	**Required on all** new offline-capable cards from **16/10/2015**	**Recommended** on all offline-capable cards		

3.2. VISA’s Mandate Principles

- SDA CAM Offline sunset announced. SDA cards in the field must be reissued from October 2018
- DDA is mandated on all Offline programs
- Online Only products are allowed in all regions for all brands in contact (in an online-only product, no SDA certificate is added in the card but issuers verify that a card is genuine based on data in the authorization requests based on a Triple DES algorithm).

Figure 7: VISA mandate overview by geography



	Europe	US	LATAM	Canada	Asia	AME
SDA CAM	Not permitted	Not permitted on new cards from 01/10/15 * Not permitted for all cards from 01/10/18** *1 January 2012 for Australia and New Zealand, 1 October 2016 for Brazil, 1 October 2018 for Japan ** 1 January 2016 for Australia and New Zealand, 1 October 2021 for Brazil, 1 October 2023 for Japan				
DDA CAM	Required on all offline-capable cards	Required on all new offline-capable cards from 01/10/2015				
CDA CAM	Optional (CDA is possible with a vendor developed VSDC application – Visa’s applet does not support CDA)					

3.3. SPA recommendation

Both VISA and MasterCard have mandated for SDA removal, starting Oct 2015. VISA and MasterCard will still allow Online Only cards (which will be mostly based on SDA chip products).

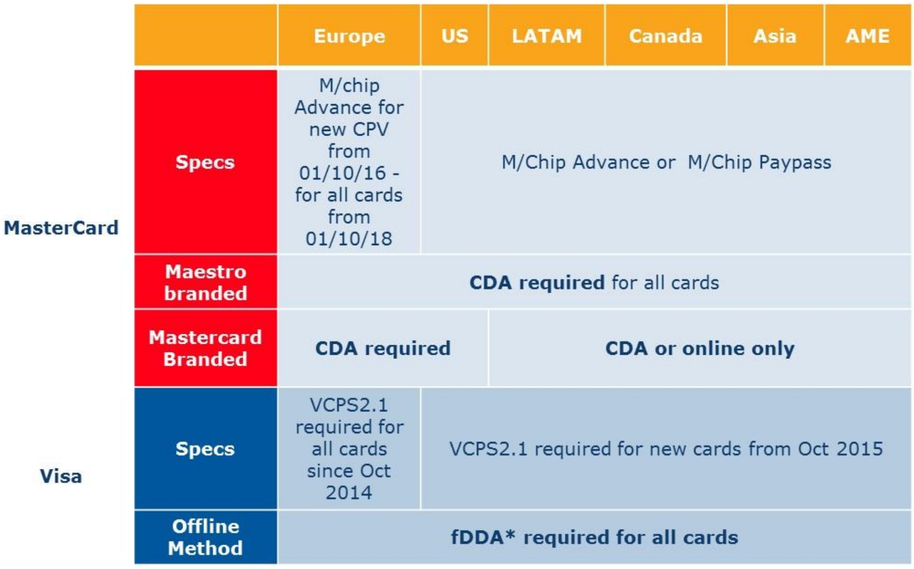
These mandates don’t necessarily mean there is a need for migration to DDA cards. In some regions VISA has recommended issuers use Online Only cards. Meanwhile, MasterCard is actively promoting DDA cards with DDA/CDA capabilities.

However, the SPA recommends the use of DDA or CDA cards for both schemes to avoid losing transactions and to ensure maximal user experience (no acceptance issue).

3.4. VISA and MasterCard Contactless Interface for Dual Interface Cards

In relation to contactless transactions, both VISA and MasterCard mandate the use of either fast Dynamic Data Authentication (fDDA) or CDA. While CDA is not being promoted nor mandated by VISA at this stage – CDA is mandated in Europe and Latin America by MasterCard.

Figure 8: VISA and MasterCard mandates for contactless cards, by geography



		Europe	US	LATAM	Canada	Asia	AME
MasterCard	**Specs**	M/chip Advance for new CPV from 01/10/16 - for all cards from 01/10/18	M/Chip Advance or M/Chip Paypass				
	Maestro branded	**CDA required** for all cards					
	Mastercard Branded	**CDA required**		**CDA or online only**			
Visa	**Specs**	VCPS2.1 required for all cards since Oct 2014	VCPS2.1 required for new cards from Oct 2015				
	Offline Method	**fDDA* required for all cards**					

**fDDA: fast DDA (See §4)*

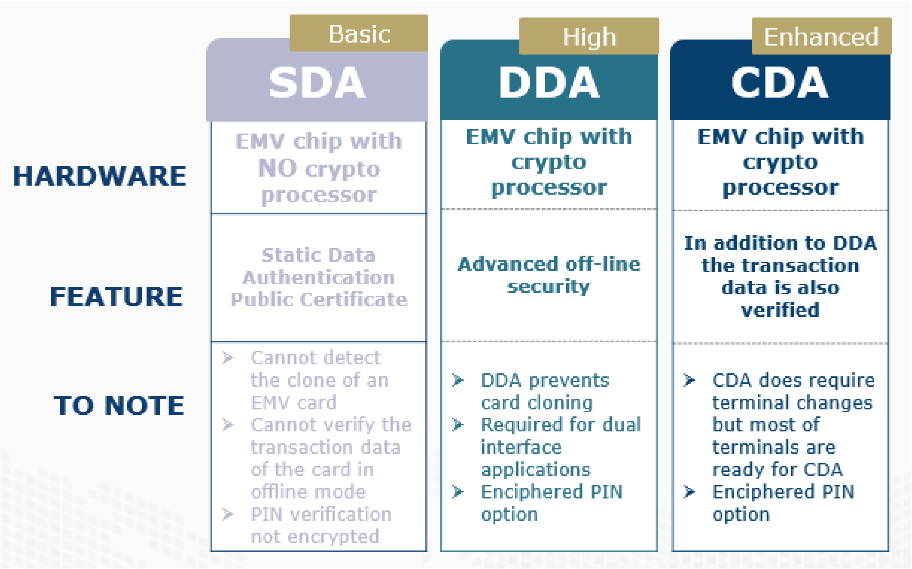
4. Definitions and Additional Insights on Authentication Methods

4.1. SDA

A certificate from the issuer is personalized on the chip card and then checked by the terminal during each transaction. The terminal verifies the correctness of the issuer's data personalized on card. If the data is proven and valid, the chip card is 'authenticated'.

This type of CAM does not require crypto-coprocessor hardware on card (a cryptographic coprocessor is a special additional processing unit in the chip that is designed to perform asymmetric or public key calculations). The card does not perform asymmetric cryptographic calculations; it only returns public application data written in public data files on the card.

Figure 8: Overview of SDA, DDA and CDA authentication features



	Basic SDA	High DDA	Enhanced CDA
HARDWARE	EMV chip with NO crypto processor	EMV chip with crypto processor	EMV chip with crypto processor
FEATURE	Static Data Authentication Public Certificate	Advanced off-line security	In addition to DDA the transaction data is also verified
TO NOTE	➢ Cannot detect the clone of an EMV card ➢ Cannot verify the transaction data of the card in offline mode ➢ PIN verification not encrypted	➢ DDA prevents card cloning ➢ Required for dual interface applications ➢ Enciphered PIN option	➢ CDA does require terminal changes but most of terminals are ready for CDA ➢ Enciphered PIN option

4.2. DDA/CDA

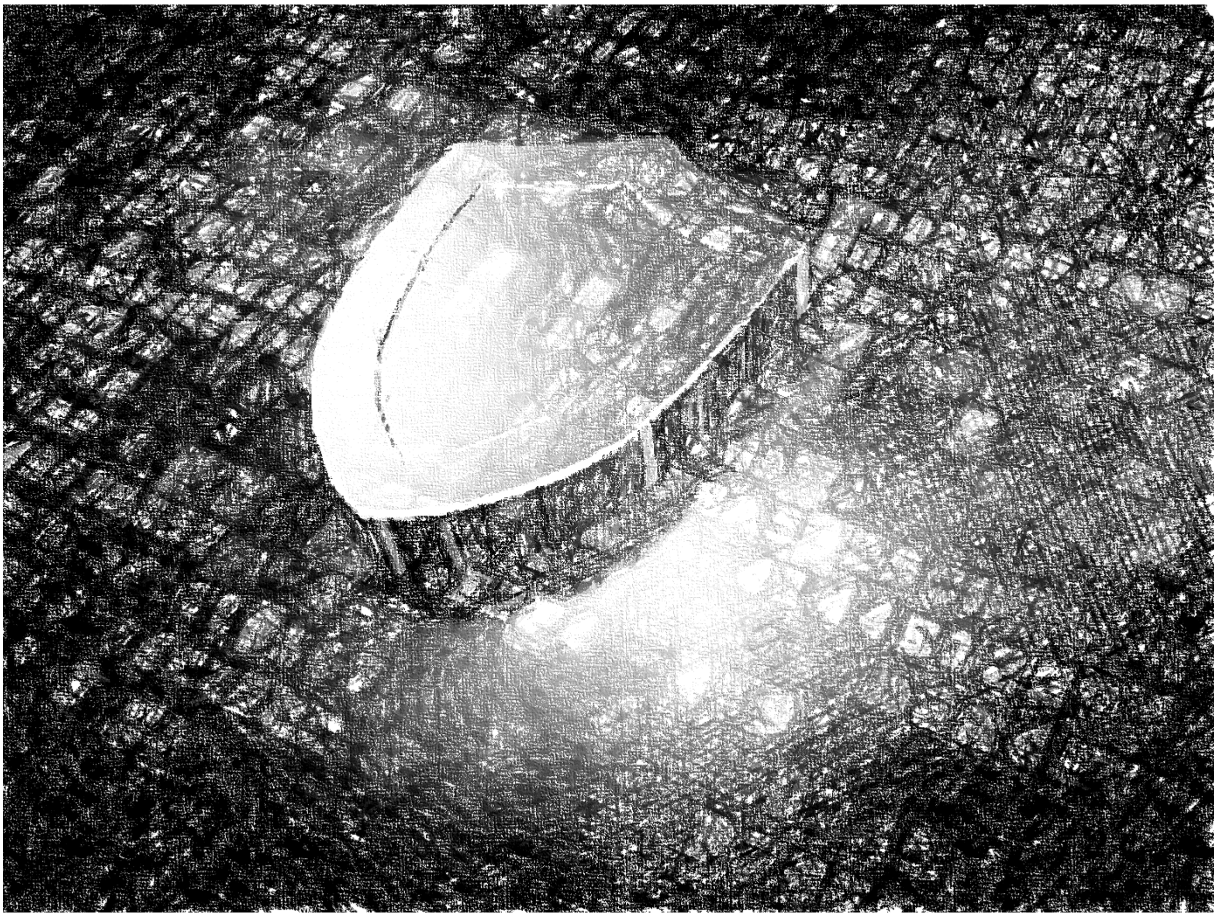
A digital signature is generated by the chip card for each transaction. The card creates a digital signature with the data, using its own secret key, and sends it to the terminal. For this activity the card needs to have a crypto-coprocessor.

The terminal checks the correctness of the dynamic signature. If the data is valid, then the card is 'authenticated´. The way the cryptography works in DDA prevents card cloning, but does not absolutely preclude a potential 'man in the middle' attack that is typically directed at the communication between the card and the terminal to trick the terminal into believing the PIN verified correctly.

A further option is CDA. This works in the same way as DDA, but also protects against so called ‘man in the middle’ attacks. During a payment transaction, the first part of the processing for CDA is the same as standard DDA. However, at a later point in the EMV transaction (during the card action analysis) the chip card generates a second dynamic signature which the terminal must verify.

4.3. fDDA

For offline contactless transactions approval, VISA has defined a different mechanism which it has named fast DDA (fDDA). This method could be considered as an equivalent to CDA, as it authenticates the main transaction-related data (the transaction amount and transaction currency).



5. DDA Evolution

In recent years DDA has become the de-facto market standard. Around 75% of EMV cards in circulation around the globe are DDA-enabled. For card issuers this means that:

- there are multiple suppliers of DDA cards, so there are plentiful offers to select from
- the difference in price is therefore lower
- all software and tests are now commonplace as an established infrastructure - labs, personalization validation tools, host systems and so forth – is in place.

In other words, making the move from SDA to DDA is straightforward as everything in the EMV environment is DDA-ready.

Technically, the main feature is the additional requirement to support a unique RSA key pair per card. The card uses this key to generate a dynamic signature for signing information communicated by the terminal. The terminal checks this signature; if the signature is valid, it is the proof that the card contains the genuine secret key and is not skimmed.

5.1. Product-Side Impacts

In addition, the non-volatile memory (the secure memory on a smart card which allows the card to hold data even after its power source is removed) required for the personalization profile is larger than for SDA.

The chips provided by chip manufacturers for DDA cards usually provide more memory size compared to those used for SDA cards. For example, a typical SDA chip used for native OS would feature 4KBytes, while the minimum memory size available for DDA chips is 8KBytes.The requirement for a crypto-processor and the larger memory size have a direct, but limited, impact on the chip required features.

Switching from SDA to DDA involves changing the type of chip used, as DDA requires a chip with a cryptographic coprocessor. This processor is necessary to perform the cryptographic calculations that allow a DDA card to generate the unique codes necessary for its trademark

5.2. Personalization-Side Impacts

From a processing point of view, the main differences regarding the personalization of DDA cards versus SDA cards are as follows.

5.2.1. Data Preparation (DP)

- A unique public/private key pair must be securely generated for each card

- In addition to the Issuer Public Key Certificate (already existent for SDA) a second new certificate – the "ICC Public Key Certificate" - is generated per card
- However, for M/Chip cards and some VSDC cards it will be necessary to generate an additional 3DES key (MKidn) using an Issuer Master Key. This key is used by the card to generate the ICC Dynamic Number that will be included in the Dynamic Signature generated during DDA processing at transaction time
- If the decision to support the "Offline enciphered PIN" option is taken, the issuer has two options for the encryption of the PIN during a payment transaction:
  - Option 1 - usage of the same card RSA key as the one used for DDA (the option most frequently used); no extra process or data to personalize than the one required for DDA
  - Option 2 -usage of a dedicated RSA key; the following new process is required
    - generation of an RSA key pair per card
    - generation of a PIN Encipherment Public Key Certificate and associated data elements.

5.2.2. Card Personalization

- The new RSA key pair must be loaded on each card
- Additional data (including the 3DES diversified key and ICC Public Key Certificate) must be loaded on each card.

5.2.3. Quality Controls

As increased layers of security are introduced with DDA, quality controls must be adapted as well.

5.2.4. Project Impacts

A set up has to be done, even for existing customers. This involves:

- a new key ceremony to exchange the new 3DES key (if needed)
- more extensive key management for the certificates and 3DES key
- script personalization needs to be updated, on the DP and electrical profiles side, depending on the customer portfolio
- a complete validation step to approve the new personalization process.

The set-up effort can vary, depending on the complexity of the customer portfolio and on the operations to be done (data preparation, key generation and so forth). These additional efforts may incur additional expenditure for the issuer.

In addition, the issuer may have to get its new personalization profile validated by the payment scheme. This is usually the case with VISA and MasterCard, which require the issuer to provide test cards for profile approval (for example, MasterCard's 'CPV – Card Personalization Validation' testing program).

5.2.5. Bank IT infrastructure impacts

Issuers that currently analyze and process SDA failure information during the authorization request will (most likely) wish to process DDA failure information. Depending on the issuer's configuration, this implies modifying the software or the parameters of the authorization server, or modifying the parameters for the on-behalf services provided by payment system networks. Optionally, a similar impact might be expected on clearing systems.

On the acquiring side, no migration is required, as years ago the two major payment systems imposed a requirement to support both SDA and DDA algorithms for offline-capable terminals.

Besides the impact on the card issuance process, a migration from SDA to DDA may have limited impacts on the issuer's IT systems.

6. Fraud and Future Protection

EMV technology has been incredibly successful in reducing fraud and offers suitable mechanisms to fight ongoing fraud and developing threats. Indeed, findings from the ECB Card Fraud Report (February 2014) demonstrate how EMV and DDA migrations have helped to combat counterfeit card fraud.

In its report, the ECB observed that, as in previous years, counterfeit fraud typically occurred in countries located outside SEPA. Although only 2% of all transactions were acquired from outside SEPA, these accounted for 25% of fraud. The disproportionately high share of cross-border fraud committed outside SEPA is mainly a result of the preference among fraudsters to exploit low security standards, such as magnetic stripe technology in the case of counterfeit fraud.

Current fraud figures, however, show that fraudsters are getting more sophisticated and will always attack any identified weak point. Consequently, anti-fraud measures must keep developing. The ECB report concludes that while ATM and POS fraud may diminish as additional countries outside SEPA migrate to EMV, CNP fraud may grow further unless appropriate mitigation measures – such as those recommended by the European Forum for the Security of Retail Payments - are adopted.

The move towards ever more secure ways to pay globally has seen DDA fast becoming an industry around the world. In 2014 DDA represented 70% of EMV card shipments globally in 2014, up 30% on 2013 figures.

DDA is a proven, state-of-the-art technology that offers a strong defense against cloning. It also expands the possibilities for secure authentication methods.

Furthermore, save for a few regional exceptions, the migration towards Dual Interface cards requires DDA too. Making the move towards DDA is therefore a necessary step for the provision of secure and sustainable payments products – both for the present and the future.

The EMV standard and underlying smart card technology has significantly upgraded transaction security levels, and DDA cards offer a higher security level for offline transactions. Fraud reduction rates in EMV countries show that issuers choosing migration to DDA have already achieved a significant milestone, emphasizing the need for EMV migration in other countries.

7. Glossary

AC	Application Cryptogram	AC is a cryptogram that is returned by the chip in response to a terminal command.
CAM	Card Authentication Method	CAM is a method to verify whether a card is genuine or not. For magnetic stripe cards, this includes the use of the hologram that can be checked by the merchant, and the presence of data on the magnetic stripe that is checked by the issuer. For chip cards, this includes the use of data contained in the chip that can be checked by the terminal of the issuer.
CDA	Combined Data Authentication	This type of CAM includes processes for offline card authentication as in DDA, and asking the card for its decision to accept or reject the transaction combined into a single command.
CPV	Card Personalization Validation	Process to ensure that a technical product has been personalized in such a manner that it is compliant with the recommendations and the mandates expressed in the appropriate documents.
DDA	Dynamic Data Authentication	This is an offline CAM technique. In this system each card has its own public/private key pair, which is created, signed, and loaded into the card by the issuer during personalization. During a transaction, the card uses its own private key to sign some data, which is transaction-dependent, which is why it is called offline "dynamic" CAM.
DES	Data Encryption Standard	The best known and most widely used symmetric cryptographic algorithm.
EMV	Europay, MasterCard, VISA	EMV is an interoperation standard for chip cards, chip capable POS terminals and ATMs, for authenticating credit and debit card payments. The name EMV comes from the initial letters of Europay, MasterCard and VISA, the three companies which originally cooperated to develop the standard.
fDDA	Fast Dynamic Data	fDDA is a data authentication mode especially designed for contactless transactions.
ICC	Integrated Circuit Card	ICC is a smart card, chip card, or integrated circuit card with embedded integrated circuits that can process data. It can receive input which is processed — by way of the ICC applications — and delivered as an output.
PIN	Personal Identification Number	PIN is a secret number; usually consists of four digits, used for the identification of a person.

ROM	Read Only Memory	Read-only memory (usually known by its acronym, ROM) is a class of storage media used in computers and other electronic devices. Because data stored in ROM cannot be modified (at least not very quickly or easily) it is mainly used to distribute firmware (software that is very closely tied to specific hardware, and unlikely to require frequent updates).
RSA	Rivest Shamir and Adleman	RSA is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.
SDA	Static Data Authentication	The simplest method of offline CAM is Static Data Authentication, or SDA. The data and signature do not vary by transaction – hence the term “static data”.

8. Sources

European Central Bank Third Report on Card Fraud – February 2014
Payments Card, and Mobile and Alaric Fraud Report – 2015
Emvco.com – 2015
Smart Payment Association 2014 annual shipments – February 2015