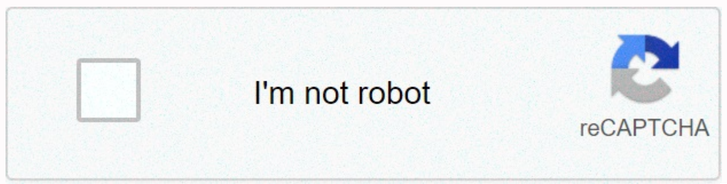

Continue

Aid on bank receipt

The U.S. may have the most complex point of sale (POS) debit payment system in the world. This can be traced back to its origin as an ATM card acceptance process, supported by multiple ATM networks. They have grown into today's sales networks (POS) with the support of large brand cards and the concept of signing debit transactions processed through credit networks. The complexity of the system can present its challenges. The trader is the top priority running their business smoothly, but it is easy to get a get ddle with the technical aspects of payment processing. In this blog post, I would like to simplify things and explain the changes that EMV has brought to the US and what it means for merchants and acquirers, especially when it comes to application identifier (AID), which helps terminal and cards communicate with each other. Magstripe vs. EMV – What has changed as a result of federal legislation in the Dodd-Frank Wall Street Reform and Consumer Protection Act (aka the Durbin Amendment), Federal Reserve Regulation II was created. This Regulation requires, inter alia, debit card issuers to support at least two competing networks when using their cards. They may include any of the global card brands or home debit networks in the U.S. The Regulation also gives traders the right to choose the network to which the transaction will be sent. For magstripe cards, it was usually selected on the processing switch – the location where the processor sends a payment authorization request to the card issuing bank. With the advent of the EMV, the processing of payments for debit transactions has become more difficult. This is due to the presence of applications on the smart card and corresponding AID in the smart card reader as opposed to limited information about magstripe cards. During an EMV transaction, if a terminal selects Global ASSISTANCE, the transaction is then rescheduled over the associated global payment network. Therefore, instead of overcrowding terminals and cards with AID for each debit network, the concept of joint US debit assistance was adopted. What is common U.S. debit assistance? Each debit card issued in the U.S. has two AID debit IDs - common U.S. debit assistance and global CARD BRAND Assistance - and each EMV-supported POS debit device has matching AID IDs to help route the transaction to the network. U.S. Common Debit Assistance can be used by all U.S. merchants who have enabled EMV debit on their POS system. The global AID brand card can be used for either American or international use. Joint ASSISTANCE allows merchants and acquirers to route the transaction to any payment network available on the card. U.S. Common Debit AID allows merchants to set up any of the global debit payment networks and debit payment networks in the U.S. that are enabled on the card, including payment networks such as Star, Accel Exchange, etc. The selection of these identifiers shall be made on the POS and, if joint debit assistance is selected, routing to any of the POS debit networks or card marks may be made at the processing switch on the basis of the cost, the amount of the transaction or any other available parameter to meet the needs of the trader. If the Global HELP tag card is selected, the processing switch must route the transaction to that particular network of card marks. SETTING THE AID preference Because the selection of the transaction routing network is transparent to the customer, traders should work with their business services or technology provider to set up a help selection during the configuration of their POS application. If you are not sure which AID to choose, you should contact your business service provider or acquirer for advice. Another important thing for traders to consider is support for PIN debit. While both the global AID card and the US Common Debit AID may support the PIN, the card can be configured with various preferred cardholder authentication (CVM) methods. Merchants who qualify for and participate in the No-CVM (small ticket) program with card marks should configure their POS application so that they do not print the signature line or send a PIN prompt for transactions that are below the supported card tag limit. If U.S. Joint Debit Assistance is selected, if the PIN is bypassed or not supported, merchants should configure their system to print the signature line on the account, or display it on signature capture devices if the allowed amount exceeds the maximum CVM allowed. Some payment solutions allow merchants or acquirers to set their AID preferences on each brand card. This allows for maximum flexibility in routing options. The use of debit, and PIN debit, is steadily increasing, especially with millennials who currently tend to prioritize over the emergence of credit card debt. Business support for pin debit is also on the rise and it is important that merchants can exercise their legal right to choose how debit transactions are processed. I hope this blog post was helpful. If you have any questions, please feel free to post them in the comments section or submit them on our Ask an Expert page. Allen Friedman is Vice President of Payment Solutions at Ingenico Group/North America This article needs additional citations for verification. Please help improve this article by adding quotes to reliable sources. Non-source material can be challenged and removed. Find sources: EMV - news · newspapers · books · scholar · JSTOR (March 2020) (Learn how and when to remove this template message) For a fun ride of the car, see the advanced motion vehicle. For Mexican Escuela Mexicana del Valle. EMV is a payment method based on the technical standard for smart card cards terminals and automated ATMs that can receive them. EMV originally stood behind Europay, Mastercard and Visa, the three companies that created the standard. EMV cards are smart cards, also called smart cards, integrated circuit cards, or IC cards that store their data on integrated circuit chips in addition to magnetic stripes for backward compatibility. These include cards that must be physically inserted or immersed in a reader, as well as contactless cards that can be read over a short distance using near-cellular communication technology. EMV-compliant payment cards are often called Chip and PIN or Chip and Signing Cards, depending on the authentication methods used by the card issuer, such as a personal identification number (PIN) or digital signature. There are ISO/IEC 7816 based standards for contact cards and ISO/IEC 14443 standards for contactless cards (Mastercard Contactless, Visa PayWave, American Express ExpressPay). In February 2010, computer scientists at Cambridge University demonstrated that the implementation of EMV PIN input was vulnerable to a mid-centre attack, but only implementations where the PIN was verified offline were vulnerable. History See also: Payment card and Chip card Until chip & PIN was in place, all personal credit or debit card transactions included the use of a magnetic stripe or mechanical fingerprint to read and record account data and signature for authentication purposes. The customer hands over his card to the cashier at the point of sale, who then hands over the card with a magnetic reader or makes a fingerprint of the increased text of the card. In this case, the system verifies the account details and prints the slip for the customer to sign. In the case of a mechanical fingerprint, transaction data is filled in, a list of stolen numbers is displayed and the customer signs the printed slip. In both cases, the cashier must verify that the customer's signature matches the signature on the back of the transaction verification card. Using a signature on a card as a verification method has several security flaws, the most obvious being the relative ease with which cards may be missing before their legitimate owners can sign them. Another involves deleting and replacing a legitimate signature, and another involves falsifying the correct signature on the card. The invention of the silicon integrated circuit chip in 1959 led to the idea of incorporating it into a plastic chip card in the late 1960s[2] The oldest chip cards were introduced as telephone cards in the 1970s [3] [4] Smart cards have since used MOS integrated circuit chips along with MOS memory technologies such as flash memory and (electrically erasable programmable read-only memory). [5] The first standard for smart cards was the Bull-CP8 Carte Bancaire M4, deployed in France in 1986, followed by the B4B0' (M4 compatible) deployed in 1989. Geldkarte in Germany also precedes the EMV. The EMV has been designed to make cards and terminals backward compatible with these standards. France has since migrated all its card and terminal infrastructure to the EMV. EMV originally stood behind Europay, Mastercard and Visa, the three companies that created the standard. The standard is now managed by EMVCo, a consortium with control split evenly between Visa, Mastercard, JCB, American Express, China UnionPay, and Discover. [6] JCB joined the consortium in February 2009, China UnionPay in May 2013,[7] and Discover in September 2013. [8] The differences and benefits of switching to smart card-based credit card payment systems are two main advantages: improved security (with associated fraud reduction) and the possibility of more subtle control of offline credit card transaction approval. One of emv's original goals was to secure multiple apps on the card: for a credit and debit card app or an electronic wallet. The new editions of debit cards in the U.S. [when?] include two applications - card associations (Visa, Mastercard, etc.) applications, and common debit applications. The common debit application ID is a little erroneous as each common debit application actually uses a resident card assignment application. [9] EMV chip card transactions improve anti-fraud security compared to magnetic stripe card transactions that rely on the cardholder's signature and visual inspection of the card to check functions such as a hologram. The use of PIN and cryptographic algorithms such as Triple DES, RSA, and SHA provide card authentication to the processable terminal and the card issuer host system. Processing time is comparable to online transactions, where communication delays account for most of the time, while cryptographic operations in the terminal take up relatively little time. The alleged increased protection against fraud has enabled banks and credit card issuers to enforce a transfer of responsibility, so that merchants are now liable (from 1 January 2005 in the EU region and 1 October 2015 in the US) for any fraud resulting from transactions in systems that are not capable of EMV. [10] [promotional source?] [11] [promotional source?] Most EMV card and terminal implementations confirm the identity of the cardholder by requiring you to enter a personal identification number (PIN) instead of signing a paper receipt. Whether or not PIN authentication takes place depends on the capabilities of the terminal and card programming. [citation needed] When introducing credit cards for the first time, merchants used mechanical rather than magnetic fingerprints that required carbon paper to make a fingerprint. They did not communicate electronically with the card issuer and the card never left the customer's eyesight. The trader had to verify transactions above a certain currency threshold by telephone of the card issuer. During the 1970s in the United States, many merchants signed up for a regularly updated list of stolen or otherwise invalid credit card numbers. This list was normally printed in the form of a newspaper paper brochure, in numerical order, similar to a slender phone book, but without any data other than a list of invalid numbers. The cashier was expected to inch through this brochure every time a credit card was presented to pay any amount, before approving a transaction that incurred a short delay. [citation needed] Later, the device electronically contacted the card issuer using magnetic stripe information to verify the card and authorize the transaction. It was much faster than before, but requires transactions to occur at a fixed location. As a result, if the transaction was not carried out near the terminal (for example, in a restaurant), the clerk or waiter had to take the card from the customer and to the card machine. It was easily possible at any time for rogue employees to swipe the card secretly through a cheap machine that immediately recorded the information on the card and stripe; In fact, even at the terminal, the thief could bend over in front of the customer and swipe the card to the hidden reader. This made illegal card cloning relatively easy, and more common occurrence than before. [citation needed] Since the introduction of the payment chip and PIN code, cloning of the chip is not feasible; only the magnetic stripe can be copied and the copied card cannot be used on its own on a terminal box requiring a PIN code. The introduction of the chip and PIN coincided with the fact that wireless data transfer technology is becoming inexpensive and widespread. In addition to mobile phone-based magnetic readers, merchant staff can now bring wireless PIN pads to the customer so the card is never seen by the cardholder. So, both chip-and-PIN and wireless technology can be used to reduce the risk of unauthorized swiping and cloning of cards. [12] Chip and PIN versus chip and signature Chip and PIN is one of two authentication methods that can use EMV-enabled cards. Instead of physically signing a receipt for identification purposes, the user simply enters a personal identification number (PIN), usually between 4 and 6 digits long. This number must correspond to the information stored on the chip. Chip and Pin technology makes it harder for fraudsters to use a card they find, so if someone steals a card, they can't make fraudulent purchases unless they know the PIN. Chip and signature, on the other hand, differs from the chip and PIN verification of the identity of the consumer by signature. Since 2015, smart and signing cards have been more common in the U.S., Mexico, parts of South America (e.g. Argentina, Colombia, Peru) and some Asian countries (e.g. Taiwan, Hong Kong, Thailand, South Korea, Singapore and Indonesia), while smart and PIN cards are more common in most European countries (e.g. THE UK, Ireland, France, Portugal, Finland and the Netherlands), as well as in Iran, Brazil, Venezuela, India, Sri Lanka, Canada, Australia and New Zealand. [13] [14] Online, telephone and mail order transactions While EMV technology has helped reduce crime at the point of sale, fraudulent transactions have shifted to more vulnerable transactions by telephone, internet and mail order , known in the industry as card or CNP transactions. [15] CNP transactions account for 20% of all credit card fraud. [16] Due to physical distance, it is not possible for the trader to present a keyboard to the customer in these cases, so alternatives have been proposed, including software approaches for online transactions that involve interaction with a card issuing bank or network website, such as Verified Visa and Mastercard SecureCode (implementation of the 3-D secure visa protocol). Create a single virtual card backed up to a physical card with a given maximum amount. Additional keyboard and screen hardware that can create a one-way password, such as a chip authentication program. Keyboard and screen integrated into the single-use password card. Since 2008, Visa has been launching pilot projects using the Emue card, where the number generated replaces the code printed on the back of the standard cards. [17] ISO/IEC 7816-3 commands define the transmission protocol between chips and readers. With this protocol, data is exchanged in application protocol data units (APDUs). This includes sending a command to a card, processing the card, and sending a response. EMV uses the following commands: Application block applications unblock card block external authenticity (7816-4) to generate cryptogram applications to retrieve data (7816-4) to obtain internal authenticity processing options (7816-4) PIN change/unblock record to read (7816-4) select (7816-4) to verify (7816-4). Commands, followed by 7816-4, are defined in ISO/IEC 7816-4 and are intermediate commands used for many smart card applications, such as GSM SIM cards. Transaction flow The EMV transaction has the following steps:[18][third-party resource required] Application selection Start processing application request Processing application data Processing restrictions offline data validation Data holder verification Verification of terminal holder Risk analysis Terminal stock analysis Stock analysis First card Online transaction permission (performed only if necessary as a result of previous steps; required at ATMs) shares of the second card Issuer Issuer Processing. The selection of ISO/IEC 7816 defines the process of selecting an application. The purpose of selecting the app was to let the cards contain completely different applications, such as GSM and EMV. However, EMV developers have implemented application selection as a way of identifying the product type, so all product witnessors (Visa, Mastercard, etc.) must have their own application. The way application selection is prescribed in emv is a common source of interoperability problems between cards and terminals. Book 1[19] of the EMV standard devotes 15 pages to describing the application process. The application identifier (AID) is used to address the application on the card or host card emulation (HCE) if it is delivered without a card. The assistance shall consist of a registered application provider identifier (RID) of five sheets issued by the registration body ISO/IEC 7816-5. The following is a proprietary extension of the application identifier (PIX), which allows the application provider to distinguish between the different applications offered. AID is printed on all EMV card holder's receipts. List of applications: Card scheme / Payment Network RID Product PIX AID Danmønt (Denmark) A000000001 Cash card 1010 A0000000011010 Visa (USA) A000000003 Visa credit or debit 1010 A0000000031010 Visa Electron 2010 A0000000032010 V Pay 2020 A0000000032020 Plus 8010 A0000000038010 Mastercard (USA) A000000004 Mastercard credit or debit 1010 A0000000041010 Mastercard[20] 9999 A0000000049999 Maestro 3060 A0000000043060 Cirrus ATM card only 6000 A0000000046000 Chip Authentication Program Securecode 8002 A0000000048002 Mastercard A000000005 Maestro UK(formerly Switch) 0001 A0000000050001 American Express (USA) A000000025 American Express 01 A00000002501 LINK ATM network (UK) A000000029 ATM card 1010 A0000000291010 CB (France) A000000042 CB (credit or debit card) 1010 A0000000421010 CB (Debit card only) 2010 A0000000422010 JCB (Japan) A000000065 Japan Credit Bureau 1010 A0000000651010 Dankort (Denmark) A000000121 Dankort 1010 A0000001211010 VisaDankort 4711 A0000001214711 Dankort (J/speedy) 4711 A0000001214712 Consorzio Bancomat (Italy) A000000141 Bancomat/PagoBancomat 0001 A0000001410001 Diners Club/Discover (USA) A000000152 Diners Club/Discover 3010 A0000001523010 Banrisul (Brazil) A000000154 Banricompras Debito 4442 A0000001544442 SPAN2 (Saudi Arabia) A000000228 SPAN 1010 A00000022820101010 Interac (Canada) A000000277 Debit Card 1010 A0000002771010 Discover (USA) A000000324 ZIP 1010 A0000000 3241010 UnionPay (China) A000000333 Debit 010101 A0000003330101010101 Credit 010102 A0000003330101020 Quasi-Loan 010103 A0000003330101030 Electronic cash 010106 A0000003330101060 ZKA (Germany) A000000359 Girocard 1010028001 A0000003591 010028001 EAPS Bancomat (Italy) A000000359 PagoBancomat 10100380 A00000035910100380 Verve (Nigeria) A000000371 Verve 0001 The Exchange Network ATM network (Canada/USA) A000000439 ATM card 1010 A0000004391010 RuPay (India) A000000524 RuPay 1010 A0000005241010 Dinube (Spain) A000000630 Dinube Payment Initiation (PSD2) 0101 A0000006300101 MIR (Russia) A000000658 MIR Debit 2010 A0000006582010 MIR Credit 1010 A0000006581010 Edenred (Belgium) A000000436 Ticket Restaurant 0100 A0000004360100 eftpos (Australia) A000000384 Savings (debit card) 10 A00000038410 Cheque (debit card) 20 A00000038420 GIM-UEMOA (Eight West African countries: Benin, Burkina Faso, Côte d'Ivoire, Guinea Bissau, Mali, Niger, Senegal, Togo) A000000337 Retrait 01 000001 A0000003373010000 Standard 01 000002 A0000003371010000 Classic 01 000003 A0000003371020000 Prepaye Online 01 000004 A0000003371011001 Prepaye Possibile Offline 01 000005 A0000003371020001 Porte Monnaie Electronique 01 000006 A0000003376010001 meeza (Egypt) A000000732 meeza Card 100123 A0000007321001 23 Initiate application processing The terminal sends the get processing options command to the card. When issuing this command, the terminal supplies the card with all the data elements required by the card in the List of Processing Options Data Objects (PDOL). PDOL (list of markers and lengths of data elements) is optionally provided by the terminal card during the selection of the application. The card responds with an Application Exchange Profile (AIP), a list of performance features when processing a transaction. The card also provides an application file locator (AFL) list of files and records that the terminal needs to read from the card. [citation needed] Read the smart card app data to store the data in your files. The AFL contains files containing EMV data. All of these must be read by using the read record command. EMV does not specify which files are stored in, so all files must be read. The data in these files is stored in BER TLV format. EMV defines tag values for all data used in card processing. [21] Processing restrictions The purpose of processing restrictions is to determine whether a card should be used. The three data elements read in the previous step are checked: Application version number, Application Usage Checker (This shows whether the card is for home use only, etc.), application effective /expiration dates check. [citation needed] If any of these checks fail, the card is not necessarily rejected. The terminal sets the appropriate bit in the terminal authentication (TVR) results, the components of which form the basis of the acceptance/rejection decision later in the transaction flow. For example, this feature allows cardholders to allow cardholders to use expired cards after their expiration date, but to make all transactions with an expired zero card online. [citation needed] Offline Authentication (ODA) Offline is a cryptographic check to authenticate a card using public key cryptography. There are three processes that can be performed depending on the card:[citation required] Static Data Validation (SDA) ensures that the data read from the card has been signed by the card ejecter. This prevents modification of the data, but does not prevent cloning. Dynamic Data Authentication (DDA) provides protection against data modification and cloning. The combined DDA/generate cryptogram (CDA) combines DDA with card application cryptogram generation to ensure card validity. CdA support may be needed in installations, as this process has been implemented in specific markets. This process is not mandatory in terminals and can only be performed if supported by both the card and the terminal. [citation needed] EMV certificates EMV certificates are used to verify the authenticity of payment cards. The EMV certification authority[22] issues digital certificates to payment card slide providers. On request, the credit card chip provides a public key certificate to the card issuer and the SSAD terminal. The terminal retrieves the certification authority's public key from on-premises storage and uses it to confirm the certification authority's trust and, if trusted, to verify that the card issuer's public key has been signed by the certification authority. If the card printer's public key is valid, the terminal uses the card printer's public key to verify that the card issuer has signed the SSAD card. [23] Cardholder verification Cardholder verification Is used to evaluate whether the person representing the card is a legitimate cardholder. Many cardholder authentication (CVM) methods are supported in the EMV. Are [citations needed] Signature Offline plaintext PIN Offline enciphered PIN offline plaintext PIN and offline signature encoded PIN and signature Online PIN No CVM required CVM failure processing Terminal uses CVM read list from card to determine type of authentication to perform. The CVM list prioritises CVM for use in relation to terminal capabilities. Different terminals support different CVMs. ATMs generally support an online PIN code. POS terminals vary in their CVM support depending on type and country. [citation needed] For offline encrypted PIN methods, the terminal encrypts the cleartext PIN block with the public key of the card before sending it to the card by using the Verify command. For the online PIN method, the cleartext PIN block is encrypted by the terminal using its point-to-point encryption key before being sent to the CPU acquirer in the authorization request message. In 2017, Emvco added support for biometric verification methods in version 4.3 of the EMV specifications[24] Terminal Risk Management Terminal Risk Management is only carried out on devices where it is decided whether the transaction should be authorised online or offline. If transactions are always carried out online (e.g. ATMs) or always offline, this step may be omitted. End-risk management is controlled by against the offline ceiling limit (above which transactions should be processed online). It is also possible to have 1 in the online counter, and check against the hot card list (which is only necessary for offline transactions). If the result of any of these tests is positive, the terminal adjusts the appropriate bit in the terminal verification (TVR) results. [25] Terminal Action Analysis The results of previous processing steps are used to determine whether a transaction should be approved offline, sent online for authorization, or offline. This is done by using a combination of data objects known as terminal action codes (TACs) in the terminal and issuer action codes (IACs) to read from the card. The TAC is logically OR'd s IAC to give the acquirer of the transaction a level of control over the outcome of the transaction. [citation needed] Both types of action code have Rejection, Online, and Default values. Each action code contains a series of bits that match the bits in the Terminal Verification (TVR) results and are used in the terminal decision whether to accept, reject, or switch online for a payment transaction. The TAC is set by the cardholder; in practice, card schemes advise TAC settings that should be used for a particular type of terminal depending on its capabilities. IAC is determined by the card issuer; some card issuers may decide that cards with an elaped zero should be rejected by setting the appropriate bit in the IAC denial. Other issuers may want the transaction to continue online in order to allow these transactions to take place in some cases. [citation needed] An online-only device, such as an ATM, always attempts to go online asking for authorisation unless it is rejected offline because of the issuer's share codes - rejection settings. During IAC processing – rejections and rejections – online-only rejections for a device is the only relevant bit of terminal authentication results, the service is not allowed. [citation needed] When an online-only device performs IAC-Online and TAC-Online processing only the relevant TVR bit, the transaction value exceeds the floor limit. Since the floor limit is set to zero, the transaction should always go online and all other values in the TAC – Online or IAC - Online are irrelevant. Online-only devices do not have to perform default IAC processing. [citation needed] First Action Analysis of the Tab One of the data objects read from the tab in the Reading application data phase is CDOL1 (Tab Data Object List). This object is a list of tags that the card wants to send to it so that it can decide whether to approve or reject the transaction (including the transaction amount, but also many other data objects). The terminal sends this data and requests a cryptogram by using the generate cryptogram command of the application. Depending on the decision of the terminal (offline, online, drop), the terminal requires one of the cryptograms from the card:[citation required] Transaction certificate (TC)— Offline cryptogram authorization request (ARQC)-Online authorization Reject Cryptogram Application Authentication (AAC)-Offline. This step gives the tab the ability to accept terminal action analysis or reject a transaction or force an online transaction. The card cannot return TC when arqc has been asked for, but can return the ARQC when tc has been requested. [citation needed] Online transactions allow transactions to be made online when arqc has been requested. The ARQC shall be sent in an authorisation report. The card generates an ARQC. Its format depends on the card application. The EMV does not specify the contents of the ARQC. An ARQC created card application is a digital signature transaction details that the card issuer can check in real time. This provides a strong cryptographic check of card authenticity. The issuer responds to an authorization request with a response code (acceptance or rejection of a transaction), an cryptogram of the authorization response (ARPC) and, optionally, an issuer script (a string of orders to be sent to the card). [citation needed] ARPC processing will not be carried out in contact transactions processed with Visa Quick Chip[26] for EMV and Mastercard M/Chip Fast[27] and in contactless transactions under schemes because the card is removed from the reader after arqc has been generated. The second action card analysis CDOL2 (Card Data Object List) contains a list of tags that the card wanted to be sent after an online authorization transaction (response code, ARPC, etc.). Although for some reason the terminal could not go online (e.g. communication failure), the terminal should resend this data to the card using the generate cryptogram authorization command. The card thus knows the issuer's answer. The card application can then reset the offline usage limits. Issuer script processing If the card issuer wants to update the card after issue, it can send card orders using the issuer's script processing. Issuer scripts are meaningless for the terminal and can be encrypted between the card and the issuer to provide additional security. The issuer's script can be used to block cards or change card parameters. [28] The processing of issuer scripts is not available in contact transactions processed with Visa Quick Chip[29] for EMV and Mastercard M/Chip Fast,[30] and for contactless transactions within systems. Control of the standard EMV contact pad for the electrical interface on the front of the credit card The first version of the EMV standard was released in 1995. Now the standard is defined and managed by emvco llc. The current members of EMVCo[31] are American Express, Discover Financial, JCB International, Mastercard, China UnionPay and Visa Inc. Each of these organisations owns share of EMVCo and has representatives in EMVCo and EMVCo working groups. Recognition of conformity with the EMV standard (i.e. device certification) shall be issued by the EMVCo on presentation of the results of tests carried out by an accredited test room. [citation needed] EMV compliance testing has two levels: EMV level 1, which includes physical, electrical and traffic-level interfaces, and EMV level 2, which includes the selection of payment claims and the processing of credit financial transactions. [citation needed] After passing the emvco joint tests, the software must be certified by payment tags to comply with the proprietary implementation of EMV, such as Visa VSDC, American Express AEIPS, Mastercard MChip, JCB JSmart or EMV-compliant implementations of non-EMVCo members such as LINK in the UK, or Interac in Canada. [citation needed] List of EMV documents and standards This section needs to be updated. Update this article to reflect recent events or newly available information. (March 2020) Since 2011, since version 4.0, official standard EMV documents defining all components in the EMV payment system have been published as four books and some other documents: Book 1: Application Independent ICC to Terminal Interface Requirements[19] Book 2: Security and Key Management[32] Book 3: Application Specification[33] Book 4: Cardholder, Requirements for operator and acquirer interface[34] Common specification of payment request[35] Emv card customisation specification[36] Versions The first EMV standard was considered in 1995 as EMV 2.0. In 1996 it was upgraded to EMV 3.0 (sometimes referred to as EMV '96) by later amendments to EMV 3.1.1 in 1998. This was further amended to version 4.0 in December 2000 (sometimes referred to as EMV 2000). Version 4.0 took effect in June 2004. Version 4.1 took effect in June 2007. Version 4.2 has been in force since June 2008. Version 4.3 has been in force since November 2011. [37] Vulnerabilities Pin collection opportunities and clonal magnetic stripes In addition to magnetic stripe data, EMV cards generally have identical data encoded on a chip that is read as part of the normal EMV transaction process. If the EMV reader is compromised to the extent that the conversation between the card and the terminal is captured, then the attacker may be able to recover both track-two data and a PIN, allowing the construction of a magnetic stripe card, which, although not usable in the chip and PIN terminal, can be used, for example, in terminal devices that allow backup magstripe processing for foreign customers without smart cards and faulty cards. This attack is only possible if (a) the offline PIN code is presented in simple text by the card input pin device, where b) the magstripe backup is allowed by the card redeemer and (c) where geographical and behavioural must not be performed by the card ejector. [citation needed] APACS, which represents the UK payments industry, claimed that the changes specified in the protocol (where card verification values differ between magnetic stripe and chip – iCVV) made this attack ineffective and that such measures would be introduced from January 2008. [38] Tests on cards in February 2008 indicated that this could be postponed. [39] Successful attacks Interception of Conversation is a form of attack allegedly carried out against Shell terminals in May 2006, when they were forced to ban all EMV authentication at their petrol stations after customers stole more than £1 million from them. [40] In October 2008, it was reported that hundreds of EMV card readers for use in Britain, Ireland, the Netherlands, Denmark and Belgium were professionally manipulated in China during or shortly there afterwards. In 9 months details and PIN credit and debit cards were sent over the mobile phone network by criminals in Lahore, Pakistan. United States National Counterinteliluation Executive Joel Brenner said previously the only national state intelligence agency would be able to pull out of this type of operation. It's scary. The data was usually used a few months after card transactions to make it harder for investigators to pin down the vulnerability. Following the discovery of the fraud, it was found that the confiscated terminals could be identified because additional circuits increased their weight by about 100 g. Tens of millions of pounds of sterling are believed to have been stolen. [41] This vulnerability has prompted efforts to introduce better control of electronic POS devices throughout their life cycle, a practice approved by electronic payment security standards such as those developed by the Secure POS Vendor Alliance (SPVA). [42] Pin collection and cloning of stripes In February 2008, BBC Newsnight programme Cambridge University researchers Steven Murdoch and Saar Drimer demonstrated one example of an attack, to illustrate that Chip and PIN are not safe enough to justify passing on responsibility to prove fraud from banks to customers. [43] [44] Cambridge University's use allowed experimenters to obtain both card data to create a magnetic stripe and PIN. APACS, the British Payments Association, disagreed with most of the report, saying the types of attacks on PIN input devices detailed in this report are difficult to carry out and not currently economically viable for a fraudster to carry out. [45] They also said that changes to the protocol (indicating the different card verification values between the chip and the magnetic stripe – iCVV) would make this attack ineffective from January 2008. The scam reported in October 2008 that worked for 9 months (above) was probably in use at the time but was not discovered for many In August 2016, computer security researchers NCR (a payment technology company) showed how credit card thieves can override a magnetic stripe code to look like a card without a chip that allows counterfeiting. [quote needed] 2010: Hidden hardware disables PIN checking on stolen Wikinews cards has related news: Chip and PIN 'not fit for purpose', says Cambridge researcher 11 February 2010 Murdoch and Drimer's team at Cambridge University announced they have found a flaw in the chip and PIN so seriously that they think it shows that the whole system needs re-writing, which was so simple that shocked them. [46] [47] The stolen card is connected to an electronic circuit and to a fake card that is inserted into the terminal (attack by a person in the middle). All four digits are entered and accepted as a valid PIN. [citation needed] A team from the BBC newsnight programme visited a Cambridge University cafe (with the consent) of the system, and were able to pay using their own cards (the thief would use stolen cards) attached to the circuit, inserting a fake card and entering 0000 as a PIN. The transactions were registered as normal and were not picked up by the banks' security systems. A member of the research team said: Even small criminal systems have better equipment than us. Indeed, the amount of technical sophistication required to carry out this attack is quite low. The vulnerability notice said: The expertise that is needed is not high (undergraduate level electronics)... We dispute the bank sector's claim that criminals are not sophisticated enough because they have already demonstrated a much higher level of skills than necessary for this attack in their miniaturized PIN input device skimmers. It is not known whether this vulnerability has been exploited. [citation needed] EMVCo disagreed and published a reply stating that, although such an attack might theoretically be possible, it would be extremely difficult and costly to successfully carry out that the current compensation checks are likely to detect or limit fraud and that the potential financial gain from the attack is minimal, while the risk of a rejected transaction or the exposure of a fraudster is considerable. [48] When approached for comment, several banks (Co-operative Bank, Barclays and HSBC) each said it was an industry-wide problem, and referred Newsnight's team to the Banking Trade Association for further comment. [49] According to Phil Jones of the Consumers' Association, Chip and PIN helped reduce card crime cases, but many cases remain unexplained. What we do know is that we have cases that are brought from individuals that seem pretty convincing. [citation needed] Because sending a PIN is suppressed, it's the exact equivalent of a merchant doing a PIN bypass Such transactions cannot succeed offline because the card never creates offline authorization without a successful PIN entry. As a result, the ARQC transaction must be submitted to an online issuer that knows that the ARQC was created without successfully filing a PIN (because this information is included in the encrypted ARQC) and would therefore be likely to drop the transaction if it were for high value, by nature, or otherwise outside the typical risk management parameters set by the issuer. [citation needed] Initially, bank customers had to prove that they were not negligent with their PIN code before obtaining redress, but the UK regulations in force since 1st [50] Murdoch said that [banks] should look back at previous transactions where the customer said their PIN had not been used and the bank record showed it had and consider refunding those customers because it could be that they are victims of this type of fraud. [quote needed] 2011: CVM downgrade allows arbitrary PIN harvest at the CanSecWest conference in March 2011, Andrea Barisani and Daniele Bianco presented research revealing a vulnerability in EMV that would allow arbitrary PIN collection despite card verification card configurations even if supported CVMs data are signed. [51] Pin collection can be carried out using a chip collector. Basically, the CVM list, which has been modified to reassue CVM to an offline PIN, is still honored with pos terminals, even though its signature is invalid. [52] The implementation of the EMV originally featured Europay, Mastercard and Visa, the three companies that created the standard. The standard is now administered by EMVCo, a consortium of financial companies. [citation needed] The most famous EMV chips are:[when?] VIS: Visa Mastercard chip: Mastercard AEIPS: American Express UICS: China Union Pay J Smart: JCB D-PAS: Discover/Diners Club International Rupay: NPCI Verve Visa and Mastercard have also developed standards for the use of EMV cards in card support devices that do not present transactions (CNP) over phone and internet. Mastercard has a chip verification program (CAP) for secure e-commerce. Its implementation is known as the EMV-CAP and supports several regimes. Visa has a Dynamic Passcode Authentication System (DPA), which is their implementation of the CAP using different default values. In many countries around the world, debit card and/or credit card payment networks have introduced liability changes. [citation needed] Normally, the card issuer is responsible for fraudulent transactions. However, if the trader's ATM or sales terminal is not supported by an EMV, the ATM owner or the trader is responsible for fraudulent transaction. Chip and PIN systems can cause problems for travelers from countries that don't issue chip and PIN cards because some retailers may refuse to accept their cards without a chip. [53] While most terminals still accept magnetic cards and require major credit card brands to accept them[54], some employees may refuse to take the card in the belief that they are responsible for any fraud if the card cannot verify the PIN code. Chip and PIN cards may also not work in some unattended vending machines, such as railway stations or self-service checkouts in supermarkets. [55] The transfer of Responsibility of Africa Mastercard between countries in the region took place on 1 January [56] By 1 January [57] The change in Visa's liability for points of sale took place on 1 January 2004. In the case of ATMs, there was a shift in responsibility 1. [58] The change in responsibility of South Africa Mastercard took place on 1 January 2007. [56] The transfer of responsibility of The Asian/Pacific Mastercard countries between countries within the region took place on 1.[56] By 1.[57] Visa's change of responsibility for points of sale took place on 1.[58] In the case of ATMs, the date of transfer of responsibility took place on 1.[59] Domestic transactions with ATMs in China are currently not subject to the transfer of commitments deadline. Australia Mastercard required all sales terminals to be EMV capable by April 2013. For ATMs, there was a shift in responsibility in April 2012. ATMs must comply with the ESM by the end of 2015[60] The shift in responsibility for ATMs took place on 1.[58] Malaysia is the first

country in the world to move fully to EMV-compatible smart cards two years after its implementation in 2005. [61] [62] New Zealand company Mastercard required all sales terminals to comply with the EMV by 1 January 2007. For ATMs, there was a shift in responsibility in April 2012. ATMs are required to comply with the ESM by the end of 2015. [60] Visa's shift in responsibility for ATMs was 1. [58] The shift in Responsibility of Europe Mastercard occurred on 1 January 2015. In the case of ATMs, liability has shifted by more than 80 % since its introduction in 1992 (see Carte Bleue). The Uk Chip and PIN UK logoChip and PIN have been tried in Northampton, England since May 2003,[63] and as a result was introduced nationwide in the United Kingdom on 14 February 2006[64] with advertisements in print and national television touted by Security in Numbers slogan. During at the first stages of deployment, if the fraudulent magnetic card transaction was deemed to have taken place, the issuing bank shall return it, as was the case before the introduction of the chip and PIN code. whereas, therefore, it is not considered that the liability for such transactions should be transferred to the retailer; this acted as an incentive for retailers to modernise their point of sale (PoS) systems and most large high street chains were modernised in time for the EMV deadline. Many smaller businesses were initially reluctant to upgrade their facilities because it required a brand new PoS system-significant investment. New cards with magnetic stripes and chips are now issued by all the big banks. Replacing pre-Chip and PIN cards was a major problem, as banks simply pointed out that consumers get their new cards when their old card expires - although many people have had cards with expiration dates until 2007. Card issuer Switch lost its main contract with HBOS on Visa because they weren't ready to issue new cards anymore at the bank it wanted. The implementation of the chip and PIN code was criticised for reducing banks' liability in cases of card fraud by requiring the customer to prove that he acted with reasonable care to protect his PIN code and card, and not from the bank that had to prove that the signature matched. Before the chip and PIN, if the customer's signature was sedated, the banks were legally responsible and had to return it to the customer. Before 1 January 1999, the Commission shall There have been numerous reports that banks have refused to pay victims of fraudulent card use, claiming their systems could not fail under reported circumstances, despite several documented successful large-scale attacks. [citation needed] The Payment Services Regulations 2009 entered into force on 1.[50] The Financial Services Authority (FSA) said: 'It is up to the bank, building society or credit card company to prove that the transaction was carried out by you and there was no failure of procedures or technical difficulties before the disclaimer. The change in liability of Latin America and mastercard between countries in the region took place on 1.[56] The transfer of Visa's responsibility for points of sale took place on 1 January 2007. In the case of ATMs, there was a shift in liability 1. [58] The change in liability of the Brazilian company Mastercard took place on 1. [56] The shift in Visa's liability for points of sale took place on 1 January 2007. In the case of ATMs [58] On 1 October 2012, Mexico Discover introduced a new directive on the transfer of responsibility of the Colombian company Mastercard. The pay at the pump at the service stations was a shift of responsibility on 1 October 2017. [66] The change in Visa's liability for points of sale took place on 1 October 2017. In the case of ATMs, there was a shift of responsibility 1. [58] The change in responsibility of Venezuela Mastercard took place on 1.[56] The transfer of Mastercard's liability to the Middle East between countries in the region took place on 1.[56] By 1 January [57] The change in Visa's liability for points of sale took place on 1 January 2007. For ATMs, there was a shift in liability 1. [58] North America Canada American Express introduced on 31 October 2015 [promotional source?] for all transactions except pay-at-the-pump at service stations; [66] [necessary third party resource] Interac (Canadian debit card network) ceased on 31 October 2017. [68] [failed verification] [third party resource needed] Mastercard introduced a shift in commitment to domestic transactions on 31 December 2017. For pay at the pump at service stations, the shift of responsibility was implemented on 31 December [67] Visa introduced a transfer of domestic transaction responsibility on 31 December 2004. For the pay at the pump at the service stations, the shift of responsibility was made on 31. [67] During the 5-year period following the migration of the EMV, the domestic card constitutes fraudulent transactions which have decreased significantly in Canada. According to Helcim reports, card-present home debit card fraud decreased by 89.49% and credit card fraud by 68.37%. [69] [promotional source?] Following widespread identity theft due to poor security at retail terminals at Target, Home Depot and other major retailers, Visa, Mastercard and Discover[70] in March 2012 – and American Express[71] in June 2012 – the United States announced its EMV migration plans for the United States. [72] Since the announcement, multiple banks and card issuers have announced cards with EMV chip-and-signature technology, including American Express, Bank of America, Citibank, Wells Fargo,[73] JPMorgan Chase, U.S. Bank, and several satellites. In 2010, several companies began issuing prepaid debit cards that contain a chip and PIN code and allow Americans to load cash as euros or pounds sterling. [74] [promotional source?] The UN Federal Credit Union was the first states of the issuer to offer chip and pin credit cards. [75] In May 2010, a press release from Gemalto (global emv card manufacturer) stated that the United Nations Federal Credit Union in New York will become the first EMV card issuer in the United States to offer its customers an EMV Visa credit card. [76] JPMorgan was the first major bank to introduce an EMV card in mid-2012, namely the Palladium card. [77] As of April 2016, 70% of U.S. consumers have EMV cards, and as of December 2016, about 50% of merchants adhere to EMV. [78] [79] However, deployment has been slow and inconsistent between suppliers. Even EMV hardware merchants may not be able to process chip transactions due to software or compliance deficiencies. [80] Bloomberg also cited problems with software deployment, including changes to sound outputs for Verifone machines, which can take several months to release and deploy software. Industry experts, however, expect greater standardization in the United States for software deployment and standards. Visa and Mastercard have introduced standards to speed up chip transactions to reduce the time for them to be under three seconds. These systems are identified as Visa Quick Chip and Mastercard M/Chip Fast. [81] On 1 January 2004, American Express introduced [82] [promotional source?] For pay at the pump, at gas stations, there is a shift of responsibility on April 16, 2021. This has been extended from 1 October 2020 due to complications caused by coronavirus. [83] 1. For pay at the pump, at gas stations, is a shift of responsibility 1 October 2020. [66] Maestro implemented the transfer of responsibility from 19. [84] Mastercard introduced 1. [82] For pay at the pump, at service stations, the change of responsibility is formally 1 October 2020. [85] In the case of ATMs, the date of change of commitment was 1. [86] [87] Visa introduced on 1 January 2020. For pay at the pump, at service stations, the change of responsibility is formal on 1 October 2020. [85] [88] In the case of ATMs, the date of the change of commitment was 1. [59] See also Contactless payments Supply chain attack Two-factor authentication MM code Reference ^ Fiat, Amos; Shamir, Adi (August 1986). How to prove it: Practical solutions to problems with identification and signature. Conference on the theory and application of cryptographic techniques. Lecture Notes in Informatics. 263rd p. 186 – 194. doi:10.1007/3-540-47721-7. ISBN 978-3-540-18047-0. S2CID 26467387. ^ Chen, Zhiqun (2000). Java Card technology for smart cards: Architecture guide and programmer. Addison-Wesley Professional. p. 3-4. ISBN 9780201703290. ^ Short smart card reviews (2019 Gemalto. 7 October 2019. ^ Sorensen, Emily (July 26, 2019). Detailed history of credit card machines. mobile transaction. October 27, 2019. ^ Veendrick, Harry J.M. (2017). Nanometer CMOS IC: From the ground up to ASIC. Springer. p. 315. ISBN 9783319475974. ^ EmvCo members. EMVCo. May 2015. ^ China UnionPay joins EMVCo (Press Release). Finextra research. They shall forthwith inform the Commission of the implementation of this Regulation. May 2015. ^ Discover joins EMVCo to help Advance Global EMV Standards. Discover network news. September 3, 2013. May 2015. ^ Visa and MasterCard support common solutions that will enable U.S. Chip debit routing. Mastercard. ^ Shift responsibility for fraudulent transactions. British Card Association. May 2015. ^ Understanding 2015 US scam liability shifts (PDF). www.emv-connection.com. EMV Migration Forum. Archived from original (PDF) 19. November 2015. ^ Why are you still not safe from fraud if you have a credit card with a chip. ABC News. ^ Chip-and-PIN vs Chip-and-Signature, CardHub.com, obtained 31 July 2012. ^ EMV Update: Discussion with the Federal Reserve (PDF). Visa. From 1 January 2017. ^ Carlin, Patricia (February 15, 2017). How to Reduce Chargebacks Without Killing Online Sales. Forbes. ^ BBC NEWS - Technology - Credit card code to fight fraud. bbc.co.uk. ^ Visa tests cards with built-in PIN machine. IT PRO. ^ How EMV (Chip & PIN) works – Transaction Flowchart. Creditcall Ltd. Acquired 10 May 2015. ^ a b Book 1: Application Independent ICC to Terminal Interface Requirements (PDF). 4.3. EMVCo. 30 November 2011. 20 September 2018. ^ MasterCard Product & Services - Documentation. From 1 April 2017. ^ EMV Chip Technology Wizard (PDF). EMVCo. November 2014. ^ EMV CA. EMV certification authority around the world. November 20, 2010. Renewed March 20, 2020. ^ Book 2: Security and Key Management (PDF). 4.3 (PDF). EMVCo. 29 November 2011. 20 September 2018. ^ ^ ContactlessSpecifications for Payment Systems (PDF). EMVCo. ^ ^ ^ ^ ^ ^ EMVCo. Members of EMVCo. August 1, 2020. ^ Book 2: Security and Key Management (PDF). 4.3. EMVCo. 29, 2011. ^ Book 3: specification (PDF). 4.3. EMVCo. November 28, 2011. September 20, 2018. ^ Book 4: Cardholder, operator, and acquirer interface requirements (PDF). 4.3. EMVCo. 27 November 2011. 20 September 2018. ^ SB CPA Specification v1 Plus Bulletins (PDF). EMVCo. 1 March 2008. 20 September 2018. ^ EMV® Card Customization Specification (PDF). EMVCo. 1 July 2007. 20 September 2018. ^ Specification of integrated circuit card for payment systems. EMVCo. March 26, 2012. ^ How safe is Chip and PIN?. BBC Newsnight. 26 February 2008. ^ Saar Drimer; Steven J. Murdoch; Ross Anderson. Pin Entry Device (PED) vulnerability. University of Cambridge Computer Laboratory. May 2015. ^ Petrol company suspends chip-a-pin. BBC News. 6 May 2006. 13 March 2015. ^ Organized crime handles European card swipe devices. The Register. 10 October 2008. ^ Technical Working Groups, Secure POS Vendor Alliance. 2009. Archived from the original 15. ^ Is Chip and Pin really safe?. BBC News. February 26, 2008. 2nd May 2010. ^ Chip and pin. 6 February 2007. Archived from the original 5. ^ John Leyden (27 February 2008). Paper buckle attack skewers Chip and PIN. Channel. May 2015. ^ Steven J. Murdoch; Saar Drimer; Ross Anderson; Mike Bond. EMV PIN verification wedge vulnerability. Computer lab, University of Cambridge. 12 February 2010. ^ Susan Watts (February 11, 2010). New flaws in the chip and pin system revealed. BBC News. 12 February 2010. ^ Responses from EMVCo to Cambridge University Report on Chip and PIN Vulnerabilities ('Chip and PIN is Broken' - February 2010) (PDF). EMVCo. Archived from original (PDF) 8. Restored on 26 March 2016. ^ Susan, Watts. New flaws in the chip and pin system have been identified (11 February 2010). Newsnight. Bbc. December 2015. ^ a b Richard Evans (October 15, 2009). Card fraud: banks must now prove their guilt. The Telegraph. May 2015. ^ Andrea Barisani; Daniele Bianco; Adam Laurie; Zac Franken (2011). Chip & PIN is definitely broken (PDF). Aperture Labs. May 2015. ^ Adam Laurie; Zac Franken; Andrea Barisani; Daniele Bianco. EMV – Chip & Pin CVM Downgrade Attack. Aperture Labs and inverse path. May 2015. ^ American credit cards outdated, less useful abroad than 'Chip and PIN' cards to grab on to. creditcards.com. [permanent dead link] ^ Visa Australia. visa-asia.com. ^ Higgins, Michelle (29. For Americans, plastic buys less abroad. The New York Times. 2017. ^ a b c d e f g h i Chargeback Guide (PDF). MasterCard around the world. November 3, 2010. May 2015. ^ and b c Operating Regulations (PDF). Visa International. Archived from original (PDF) 3. ^ a b c d e f g (i) Path to dynamic data. Visa. [permanent dead link] ^ and b Visa extends the U.S. plan for EMV Chip adoption to include ATM and Common Debit Solutions (Press Release). Foster City, Calif.: Visa. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive May 2015. ^ and b MasterCard announces a five-year plan to change the face of the payments industry in Australia. Mastercard Australia. Archived from the original 28. ^ Malaysia first to complete chip-based card migration. Start online. ^ Usa learns from Malaysia, 10 years later. October 14, 2015. ^ Anti-credit card fraud in court. BBC Business News. On 11 April 2003. May 2015. ^ British Card Association. Chip and PIN Wizard (PDF). May 2015. ^ Foundation, Internet memory. [ARCHIVED CONTENT] UK Government Web Archive - National Archives. Archived from the original on April 12, 2017. ^ and b c Discover to enforce EMV accountability shift to 2015 (Press Release). Finextra research. November 12, 2012. May 2015. ^ a b c Chip Accountability Shift. global payments. Archived from the original 30. ^ Interac - For traders. April 2017. ^ EMV reduces card-current fraud in Canada (Infographic) - Official Helcim™ Blog. From 1 April 2017. ^ Discover implements the EMV mandate for the U.S., Canada and Mexico. Archived from the original 10. ^ American Express announces US EMV plan to advance contact, contactless and mobile payments (Press Release). New York: American Express. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and Archived from the original 10. May 2015. ^ EMV is uncertain fate in the U.S. Protean payments. Archived from the original on 29 September 2012. ^ Camhi, Jonathan (August 3, 2012). Wells Fargo introduces a new EMV card for consumers. Bank Systems & Technology. Archived from the original 5. May 2015. ^ Travelex Offers America's First Chip & PIN Enabled Prepaid Foreign Currency Card. Commercial wire. Commercial wire. 1 December 2010. Unfcu will be the first U.S. issuer to offer high-security credit cards. United Nations Federal Credit Union. ^ Ray Wizbowski (May 13, 2010). The United Nations Federal Credit Union will select Gemalto for the first U.S. issued globally compliant credit card (Press Release). Austin, Texas: Gemalto. May 2015. ^ Paul Riegler (July 25, 2013). Chip-and-Pin and Chip-and-Signature Credit Card Primer for 2013. Frequent Business Traveler. May 2015. ^ Goldman, Sharon (March 20, 2017). Is the rocky road to EMV retail adoption getting smoother?. April 2017. ^ EMV Credit Card Poll. ^ Retailers have smart card readers - why don't they use them?. November 2017. ^ Plan to chip credit cards less Bloomberg.com July 2017. August 2017. ^ and b Cathy Medich (July 2012). EMV Migration - powered by payment brand Milestones. May 2015. ^ Amex joins Visa in postponing U.S. gas migration EMV. ^ David Heun (September 10, 2012). MasterCard brings EMV Chip-Card liability policies to U.S. ATMs. SourceMedia. Archived from the original on 22 February 2014. May 2015. ^ and b EMV Fuel Responsibility Delay Pumps card scams concerns. Credit Union Times. December 2016. ^ Beth Kitchener (10. MasterCard extends EMV migration plan in U.S. to ATM Channel (Press Release). Purchase, N.Y.: Mastercard. May 2015. ^ EMV for U.S. acquirers: Seven guiding principles for EMV readiness (PDF). Archived from original (PDF) April 5, 2017. ^ Visa announces U.S. participation in the Global Point-of-Sale Counterfeit Liability Shift (PDF) (Press Release). Visa. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive May 2015. External Links Official Site Why EMV Chip is used in debit/credit cards. Obtained from 2 Cannot be confused with the card security code. 3-D Secure is a protocol designed to be an additional security layer for online credit and debit card transactions. The name refers to three domains that interact using the protocol: merchant/acquirer domain, issuer domain and interoperability domain. [1] It was originally developed by Arcot Systems (now CA Technologies) and Visa[2] with the intention of improving the security of Internet payments and offered to customers under the Visa-verified brand name. Protocol-based services have also been adopted by MasterCard as SecureCode, appearing as ProtectBuy,[3] JCB International as J/Secure, and American Express as American Express SafeKey. [4] Later, Emvco carried out later revisions of the protocol under the name EMV 3-D Secure. Version 2 of the Protocol was published in 2016 in order to meet the new EU authentication requirements and to address some of the shortcomings of the original protocol. [5] An analysis of the first version of the protocol by academia has shown that it has many security issues affecting consumers, including a larger area for phishing and a shift in liability in the case of fraudulent payments. [6] Description and essential aspects This section does not mention any resources. Please help improve this section by adding citations to reliable sources. Non-source material can be challenged and removed. (March 2010) (Learn how and when to delete this message template) The basic concept of the protocol is to tie the financial authorisation process to online authentication. This additional security validation is based on a model of three domains (that is, 3-D in the name itself). Three domains are: Domain Acquirer bank and the merchant to whom the money is paid). Domain of the issuer (the bank that issued the card used). Interoperability domain (infrastructure provided by a card scheme, credit, debit, prepaid or other types of credit card to support the 3-D Secure Protocol). Includes The Internet, Merchant Add-on, Access Control Server, and other software providers The protocol uses XML messages sent over SSL connections with client authentication[7] (this guarantees the authenticity of both partners, the server, and the client using digital certificates). A transaction using a verified visa or SecureCode initiates a redirection to the card bank's website to authorize the transaction. Each issuer can use any kind of verification method (the protocol does not apply), but usually a card-based password is entered for online purchases. The Visa Verified protocol recommends that the bank's verification page be loaded in a nested frame session. In this way, the bank's systems can be responsible for most security breaches. Today it is easy to send a one-time password as part of sms text messages to users' mobile phones and emails for authentication, at least during registration and forgotten passwords. The main difference between the implementation of Visa and Mastercard lies in the method for generating UCAF (Universal Cardholder Authentication Field): Mastercard uses AAV (Accountholder Authentication Value) and Visa uses CAVV (Cardholder Authentication Verification Value). [clarification needed] 3-D Secure Flow ACS Providers In the 3-D Secure protocol, the ACS (access control server) is on the issuer(s) side. Currently, most banks outsource ACS to a third party. The buyer's web browser normally displays the domain name of the ACS provider and not the bank domain name; However, the protocol does not require this. Depending on the ACS provider, you can specify a bank-owned domain name for use in the ACS. MPI providers Each 3-D Secure Version 1 transaction includes two request/internet response pairs: VEReq/VERes and PAReq/PARes. [8] Visa and Mastercard do not allow merchants to send requests directly to their servers. Traders must instead use merchant plug-in (MPI) providers. Traders This section does not list any resources. Please help improve this section by adding citations to reliable sources. Non-source material can be challenged and removed. (March 2010) (Learn how and when to delete this message template) The advantage for traders is the reduction of chargebacks of unauthorized transactions. One of the disadvantages for traders is that they must buy a business plug-in (MPI) to connect to a Visa or Mastercard directory server. This is an expensive [necessary clarification] (installation fee, monthly fee and transaction fee); also represents additional revenue for Providers. 3D security support is complex and occasionally creates transaction failures. Perhaps the biggest disadvantage for traders is that many users perceive the additional authentication step as a nuisance or impediment, resulting in a substantial increase in abandonment of transactions and loss of revenue. [9] Buyers and credit card holders This section does not mention any resources. Please help improve this section by adding citations to reliable sources. Non-source material can be challenged and removed. (September 2011) (Learn how and when to delete this message template) In most current implementations of 3-D Secure, the issuing bank or its ACS provider prompts the buyer for a password that is known only to the bank/ACS provider and the buyer. As the trader does not know this password and is not responsible for intercepting it, it can be used by the issuing bank as proof that the buyer is indeed their card holder. The aim is to help reduce the risk in two ways: Copying card data, either by registering numbers on the card itself or through modified terminals or ATMs, does not result in the possibility of buying over the Internet because of an additional password that is not stored on the card or written on the card. As the trader does not capture the password, there is a reduced risk of security incidents for online traders; Although the incident may result in hackers getting additional card data, there is no way to get the associated password. 3-D Secure does not strictly require the use of password authentication. They say it is possible [quotes to be] used in conjunction with smart card readers, security chips and the like. These types of devices can provide customers with a better user experience by exempting the buyer from using a secure password. Some issuers now use such devices as part of a chip authentication program or dynamic passcode authentication systems. [citation needed] One significant drawback is that cardholders are likely to see their browser join unknown domain names due to suppliers' MPI implementations and the use of externally ACS implementation by issuing banks, which could facilitate the execution of phishing attacks on cardholders. General criticism Site identity verifiability The system includes a pop-up window or nested frame that appears during the online transaction process, requiring the cardholder to enter a password, which, if the transaction is legitimate, their card issuing bank will be able to verify. The problem for cardholders is determining whether a pop-up window or frame is really out of their card issuer when it could be from a fraudulent website trying to harvest card details. Such script-based pop-ups or frames do not have access to any security certificate, eliminating implementation of the 3-DS. The Visa-Verified system has earned some criticism[10][11][12][13] because it is difficult for users to distinguish between a legitimate visa-verified pop-up window or a nested frame and a fraudulent phishing site. This is because the pop-up window is served from the domain that is: It's not where the user buys not the card issuing the bank Not visa.com or mastercard.com In some cases, the verified-by-Visa system has been exchanged by users for phishing scam[14] and itself has become the target of some phishing scams. [15] A newer recommendation to use an inline frame (iframe) instead of a pop-up has reduced user confusion at the cost of complaining, if not impossible, for the user to verify that the page is genuine in the first place. Since 2011,[needs updating] most web browsers do not provide a way to check the security certificate for iframe content. Some of these concerns about the validity of the site for verified-by-Visa are alleviated, however, as its current implementation of the registration process requires entering a personal message that appears in the later Verified-by-Visa pop-up to provide some certainty to the user the pop-ups are genuine. [16] Some cardholders also use activation during shopping (ADS),[17] in which cardholders who are not registered with the system are offered the possibility to register (or be forced to log in) during the purchase process. This usually gets them into a form that is expected to confirm their identity by answering security questions that should be known to their card-deeders. Again, this happens within an iframe where they can't easily verify the sites that provide this information-cracked site or an illegitimate marketer could in this way gather all the details they need to pose as a customer. The implementation of the 3-D Secure sign-up often does not allow the user to continue purchasing until they have agreed to sign 3-D Secure and its terms, which offers no alternative way to navigate from the site to close it, thus suspending the transaction. Cardholders who are unwilling to risk registering their card during a purchase, with the business site controlling the browser to some extent, may in some cases go to their bank's home page on the web in a separate browser window and register from there. When they return to the business site and start over, they should see that their card is registered. The presence on the personal insurance message (PAM) password page they chose at check-in confirms that the page comes from a bank. This still leaves some possibility of a man-in-the-middle attack if the cardholder cannot verify the SSL server certificate for the password page. Some business sites will devote the entire browser page to verification than using a frame (not necessarily an iFrame), which is a less secure object. In this case, the lock icon in the browser should show the identity of the bank or the operator of the verification point. The cardholder can confirm that it is in the same domain that he/she visited when registering his/her card, unless it is the domain of their bank. Mobile browsers pose particular problems for 3-D Secure, due to the common lack of some features such as frames and pop-up settings. Even if the trader has a mobile website, if the issuer is also mobile-aware, the verification pages may fail to render correctly or even at all. Finally, many [vágni] analysts have concluded that activation protocols during shopping (ADS) pose a greater risk than they eliminate and, in addition, transmit this increased risk to the consumer. In some cases, 3-D Secure ends up providing little security for the cardholder, and may act as a device to transfer responsibility for fraudulent transactions from the bank or retailer to the cardholder. The legal conditions applicable to 3-D Secure are sometimes formulated in a way that makes it difficult for the cardholder to escape liability from fraudulent transactions by the cardholder who is not present. [18] Geographical Discrimination Banks and Merchants may use 3-D Secure systems unevenly with respect to banks issuing cards in multiple geographic locations, thus creating a differentiation, for example, between domestic cards issued in the USA and outside the USA. For example, because Visa and Mastercard treat the unregistered U.S. territory of Puerto Rico as a non-U.S. international, rather than domestic location in the U.S., cardholders there may face a greater incidence of 3-D Secure queries than cardholders in fifty states. Complaints to that effect were received by the Puerto Rico Department of Consumer Affairs equal treatment of economic discrimination sites. [19] 3-D Secure as strong customer authentication version 2 3-D Secure, which contains one-time passwords, is a form of software strong customer authentication as defined in the revised EU Payment Services Directive (PSD2); previous variants have used static passwords which are not sufficient to meet the requirements of the Directive. 3-D Secure relies on the issuer to be actively involved and to ensure that each card issued is registered by the cardholder; as such, acquirers must either accept unpacked cards without performing strong customer authentication, or reject such transactions, including transactions from smaller card schemes that do not have 3-D Secure implementations. Alternative approaches shall carry out verification on the acquisition side without requiring prior registration with the issuer. For example, patented authentication [20] of PayPal uses one or more fictitious credit card transactions and the cardholder must value of these transactions, although the verification cannot be directly related to a specific transaction between the merchant and the cardholder. A patented[21] system called iSignthis divides the agreed transaction amount into two (or more) random amounts, with the cardholder then demonstrating that he is the account holder by confirming the amounts on their statement. [22] ACCC Blocks 3-D Safe Draft 3-D mandatory security proposal in Australia has been blocked by the Australian Competition and Consumer Commission (ACCC) after receiving numerous objections and submissions related to errors. [23] India Some countries like India have used not only CVV2, but 3-D Security mandatory, SMS code to send from the bank and entered into the browser when you are redirected, when you click the purchase button to the payment system or banking system page where you enter this code and only then the operation is accepted. Yet Amazon can still make transactions from other countries with 3-D security turned on. [24] 3-D Secure 2.0 In October 2016, Emvco published a specification for 3-D Secure 2.0; it is designed to be less intrusive than the first version of the specification, allowing more contextual data to be sent to the client's bank (including postal addresses and transaction history) in order to verify and assess the risk of the transaction. A customer would only be required to pass an authentication challenge if their transaction is identified as high risk. In addition, the authentication procedure is designed to no longer fit the redirection to a separate page and can also activate off-line authentication via the institution's mobile application (which in turn can also be used with biometric authentication). 3-D Secure 2.0 is in line with eu mandates for strong customer authentication. [5] [25] [26] See also Secure Electronic Transaction (SET) Merchant Plug-in (MPI) References ^ ^ Visa USA Tightens Security with Arcot. Zdnet. ^ ProtectBuy. discover.com. ^ SafeKey. AmericanExpress.com. Archived from the original for 2011-08-07. Loaded 2010-08-11.^ and b Traders cannot let 'PSD2' and 'SCA' be vague initials. PaymentsSource:Supplied Loaded 2019-07-11. ^ Verified Visa and MasterCard SecureCode: or, How not to suggest authentication (PDF). ^ 202008%20fsdfgsd/3D_Secure_Emre_Kaplan.pdf ^ Verified Visa Implementation Guide (PDF). ^ Are Visa and MasterCard SecureCode certified conversion killers?. practicalecommerce.com. Acquired 2013-07-30. This 2010 study documented an increase in the number of abandoned transactions by 10% to 12% for traders newly joining the program. ^ Antiworm: Verified Visa (Veriphied Phishing?). Antiworm.blogspot.com. 2006-02-02. Loaded 2010-08-11. ^ Muncaster, Phil. Industry sets up 3-D Secure - 11 April 2008. IT week. Archived from the original for 2008-10-07. 2010-08-11. ^ Brignall, Miles (2007-04-21). A verified visa system has shaken thousands of shoppers online. The Guardian. London. Archived from the original 6. Loaded 2010-04-23. ^ Verified Visa and MasterCard SecureCode: or, How not to suggest authentication (PDF). Loaded 2010-08-11. ^ securesuite.co.uk phishing scam?. Ambrand.com. Acquired 2010-08-11. ^ Verified Visa Activation - Visa Phishing Scams. MillerSmiles.co.uk. 2006-08-22. Archived from the original 8. Loaded 2010-08-11. ^ Verified Visa FAQ. www.visa.co.uk. October 2016. ^ Activation while shopping (PDF). Visaeurope.com. Acquired 2010-08-11. ^ Verified Visa and MasterCard SecureCode: or, How not to suggest authentication (PDF). Loaded 2012-04-23. ^ daco.pr.gov. daco.pr.gov. Archived from the original for 2014-08-12. Loaded 2014-07-17. ^ US2001021725 System and method for verifying the financial instrument. Patentscope.wipo.int. 2002-01-17. Loaded 2014-07-17. ^ AU2011000377 Transaction authentication methods and systems. Patentscope.wipo.int. Acquired 2014-07-17. ^ EPCA Payment Summit: iSignthis presents its authentication service as an alternative to 3D Secure. Payday. Loaded 2014-07-17. ^ The ACCC releases a draft decision against ordered use of 3D secure for online payments. ^ Amazon.in Help: About CVV and 3-D Secure. www.amazon.in. In 2020-06-17, a secure password was required by the Reserve Bank of India to ensure safer online shopping. This will prevent misuse of the lost/stolen card because the user will not be able to continue unless he enters the password associated with your card, created by you and known only to you. ^ Adyen Touts His 3-D Secure 2.0 Service First Launch. digital transactions. Loaded 2019-07-11. ^ Deity, Olivier. Stripe: 3D Secure 2 - Guide to 3DS2 Authentication. Stripe. Loaded 2019-07-11. External links American Express SafeKey (consumer site) American Express SafeKey (global partner site) Verified Activation visa verified Visa Partner Network Mastercard SecureCode home page usa.visa.com Discover Global Network ProtectBuy obtained from