Universidade Estadual de Campinas – UNICAMP
Instituto de Computação - IC
Mestrado Profissional em Computação

Segurança em cartões Smartcard EMV

Ricardo Barbosa Matsuno - RA – 022532
Marcelo Chaves - RA – 890735

Índice

1. Introdução

A utilização de cartões bancários, tanto crédito ou débito, vêm crescendo anualmente, no entanto, em paralelo a fraude neste tipo de sistema é cada vez maior.

Hoje em dia a maioria dos meios de pagamentos eletrônicos ainda utilizam a tecnologia de cartões magnéticos para a realização de transações de transferência Eletrônica de fundos, no entanto o cartões magnéticos estão cada vez mais suscetíveis à fraudes, sendo que com um mínimo de conhecimentos técnicos uma pessoa hoje em dia é capaz de realizar a clonagem de cartões. Aparelhos que copiam cartões magnéticos podem ser comprados em qualquer loja de informática indiscriminadamente.

Para combater a fraude crescente no cartões magnéticos, muito bancos e administradoras de cartão de crédito estão migrando para novas tecnologias baseadas em SmartCards, cartões inteligentes microprocessados, e que além de muito mais difíceis de se clonar que um simples cartão magnético, oferece uma série de mecanismos de segurança adicionais.

Pensando nisso a Visa, Mastercard e Europay criaram a norma EMV, para cartões inteligentes, aonde são definidos todos os mecanismos de segurança e toda a inteligência não somente dos cartões, mas de todo uma transação eletrônica, desde o cartão, terminais de captura de transações, até a autorização dos emissores.

Neste trabalho vamos detalhar o funcionamento de uma transação realizada sob as normas EMV, dando ênfase aos mecanismos de segurança definidos pela norma.

2. Sistema baseado em cartões magnéticos

A maioria dos sistemas de transferência eletrônica de fundos está baseada em cartões magnéticos que são processados online. São sistemas muito simples e que provêem poucos mecanismos de segurança.

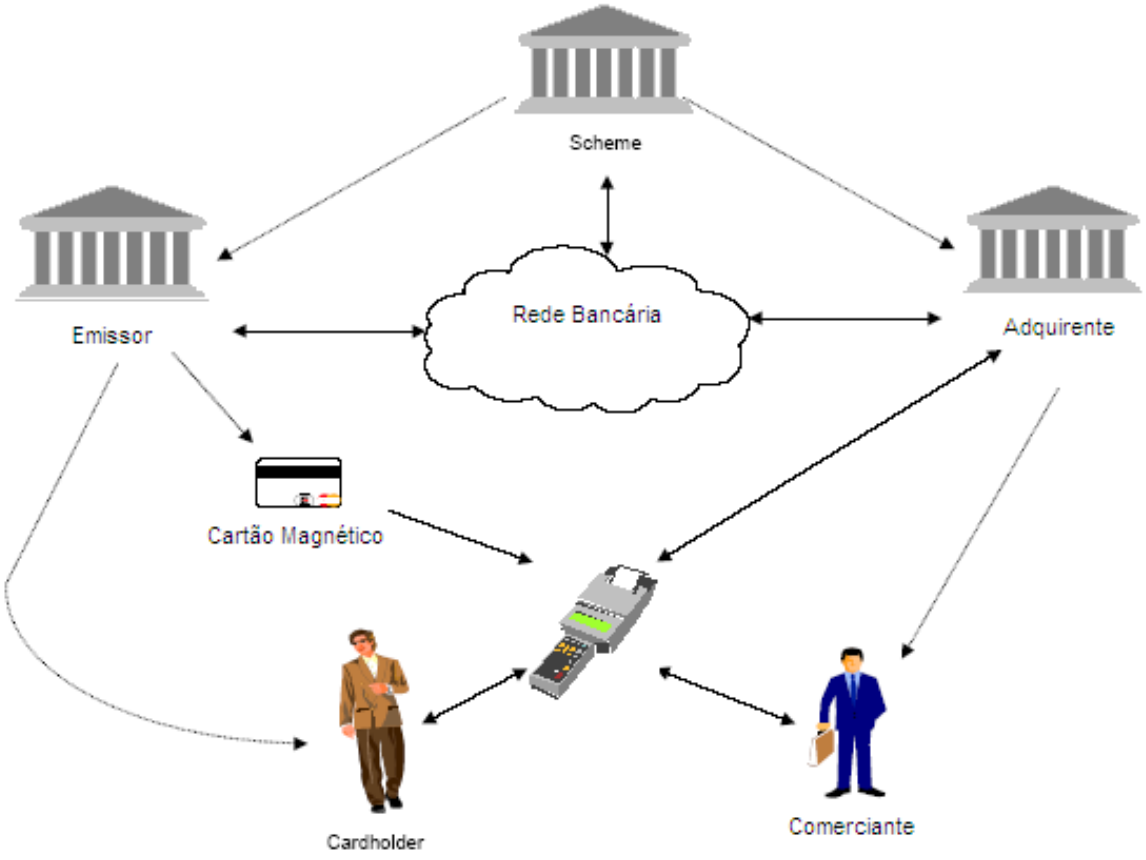

Fig1 – Sistema baseado em cartões magnéticos

Como principais características deste tipo de sistema, temos:

- Autorizações online
- Autenticação de usuários visualmente ou através da senha online
- Alto índice de fraudes, realizadas através da clonagem de cartões magnéticos.

Na tabela abaixo podemos ver resumidamente os processos de segurança existentes neste sistema.

Processo	Método
Autenticação / validação do cartão	Autenticação Visual – utiliza quase os mesmos mecanismos descrito mais adiante na parte de cartões SmartCard
Autenticação do usuário do cartão	Através de assinatura ou senha online
Autenticação do emissor do cartão	Não existe
Autenticação da transação	Não existe

Este sistema está sujeito a uma série de ataque como :

- Roubo de cartões – como o principal mecanismo de segurança da maioria dos é baseado em processos manuais/ humanos como autenticação visual (validação da assinatura do cartão) e portanto sujeita a muitas falhas. O que torna possível para o ladrão executar operações com o cartão , pelo menos até que o proprietário comunique o roubo
- Clonagem de cartões – A cópia de cartões magnéticos pode ser realizada facilmente além de não requerer quase nenhum conhecimento especializado para realizar a mesma.
- Repúdio de transações – Como não existem mecanismos para autenticar as transações, muitas vezes é complicado contestar o repúdio de transações.

3. Sistema EMV

Em 1996, as bandeiras de cartão de crédito se uniram para criar uma norma de cartões inteligentes, que acabou sendo denominada EMV (referência à Europay, Mastercard e Visa) . Desta forma seria possível criar um sistema baseado em cartões inteligentes e que proporcionasse a mesma interoperabilidade de sistemas e equipamentos que existe atualmente com os cartões de crédito.

Já desde muitos anos, foram criados os chamados cartões inteligentes, que oferecem muito mais recursos e segurança, e desde então são considerados os substitutos naturais para os cartões magnéticos, mas no início devido ao alto custo dos cartões ainda não era economicamente justificável a migração, era mais vantajoso conviver com as fraudes do sistema baseado em cartões magnéticos. No entanto com o aumento das fraudes, da utilização de cartões e da redução do custo de um SmartCard, a tecnologia se viabilizou economicamente.

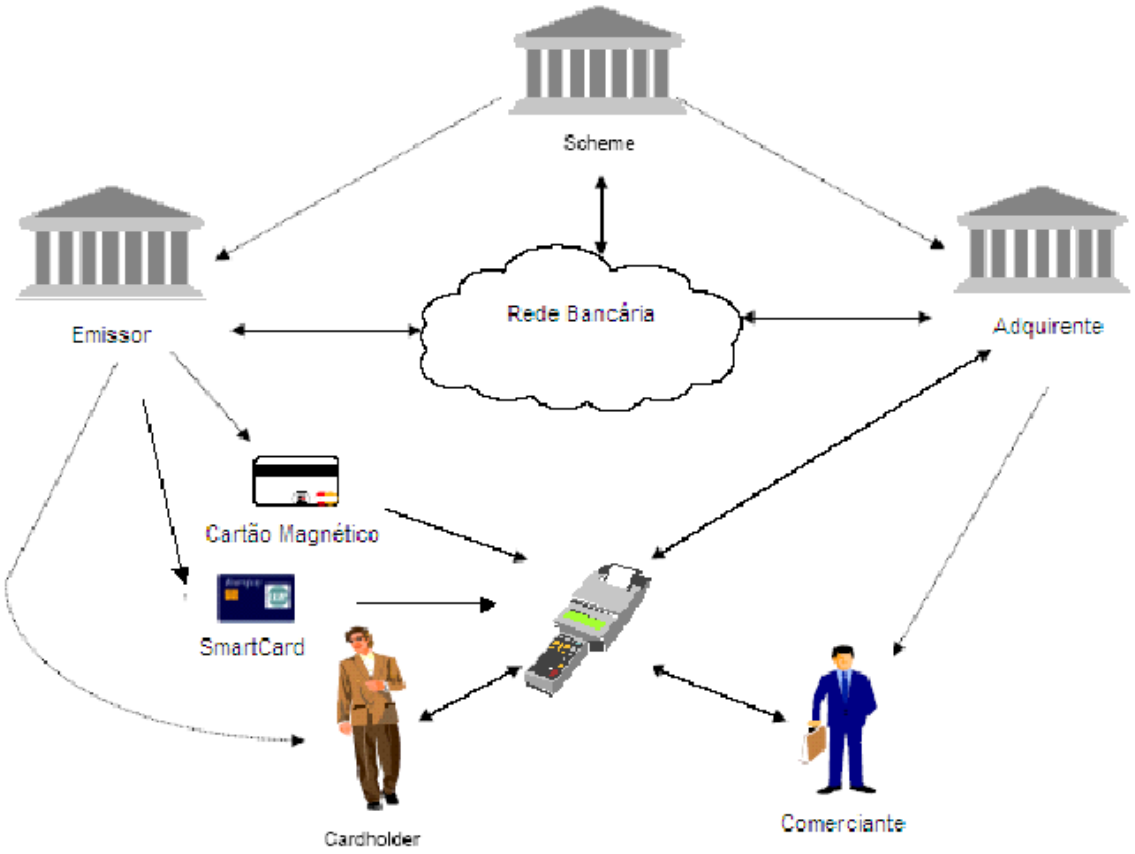

Fig2 – Sistema baseado em cartões inteligentes

A arquitetura do sistema em geral não sofre muitas modificações, os principais atores seguem existindo, sendo que as maiores mudanças serão dentro do processamento de cada componente.

3.1. Cartões inteligentes

Os cartões inteligentes surgiram na França em 1974 por definição, o cartão inteligente é definido como um cartão microprocessado com uma memória RAM, EPROM e EEPROM, ligados a um canal serial de entrada e saída.

Os cartões possuem vários componentes de segurança [6] , dentre eles podemos destacar :

- Características de Segurança Visual – Através de características visuais é possível oferecer alguns mecanismos que dificultam sua cópia ou modificação. Tais características são basicamente :
  - Assinatura do portador –
  - Hologramas –hologramas presentes no cartão e que não podem ser retirados sem danificar o cartão e o holograma.
  - MicroImpressão – Linhas ultrafinas que são invisíveis ao olho nu,mas que visíveis se ampliadas.
  - Embossing – a impressão em alto relevo dos dados do portador do cartão
  - Padrões de segurança – este processo é conhecido como “guiloche”, e se baseia na impressão de pequenas linhas entrelaçadas no corpo do cartão
  - Gravura a laser –
- Caraceterísticas de segurança do chip
  - Durante a produção de um chip de SmartCard, após o teste dos microcircuitos, o chip deve passar a um estado irreversível , aonde é impossível acessar os circuitos internos do chip.
  - Outra característica de segurança é colocar os componentes do circuito do chip nas camadas mais baixas do silício, de forma a prevenir engenharia reversa do S.O do chip.
  - Para prevenir o monitoramento de sinais elétricos pelas células de memória, existe uma área da memória protegida por um escudo de metal, sendo que a remoção do mesmo destrói o circuito.
  - Circuitos para detectar invasões externas. Estes circuitos controlam se a tensão é muito alta ou muito baixa, freqüências de clock muito alta ou muito baixa, e muitas vezes sensores de temperatura.
- Características de segurança do S.O do cartão.
  - Todo o acesso à memória é realizado pela CPU,o que torna o S.O. um componente crítico de segurança do cartão .

- O acesso à diretórios e arquivos do cartão podem ser protegidos por Senhas pessoais , ou/e chaves criptográficas. Se uma senha é entrada incorretamente, após um certo número de vezes o cartão pode ser bloquado.

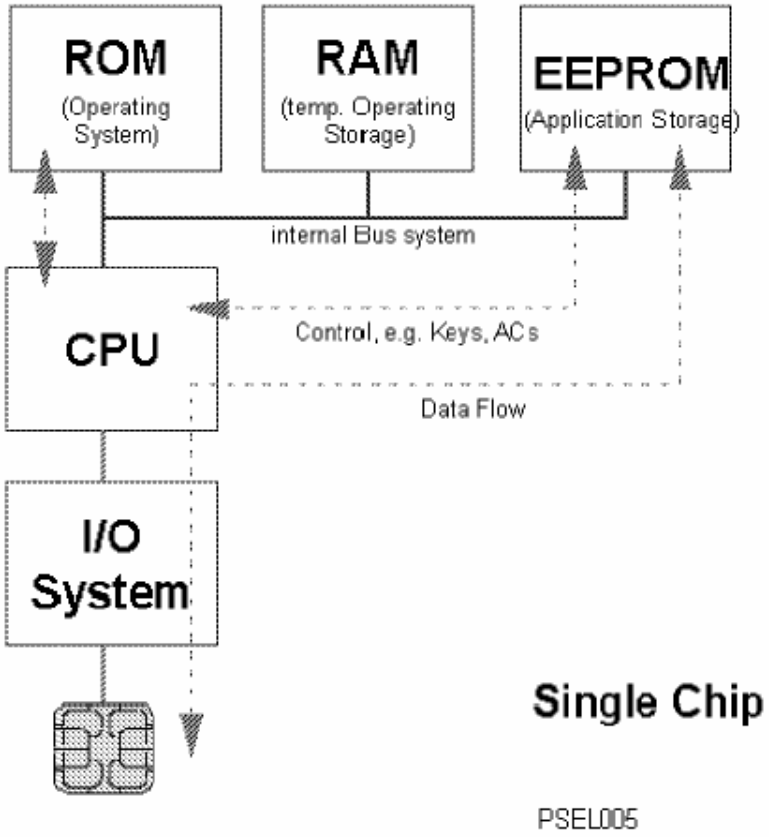

Fig 3 Arquitetura interna de um SmartCard [6]

3.2. Protocolos de segurança EMV

Uma operação financeira realizada com um cartão EMV, está protegida por diversos mecanismos de autenticação e verificação definidos pela norma EMV.

Os principais mecanismos de segurança são :

- Protocolos de autenticação do cartão – A norma define mecanismos para autenticar os dados presentes em um cartão EMV.
- Protocolos de autenticação do usuário – como autenticar e validar o portador do cartão .
- Protocolo de autenticação da transação – processo de autenticação das transações realizadas pelo cartão
- Protocolo de autenticação do emissor – processo de autenticação do emissor.

Para a realização de todas estas autenticações e validações, a EMV utiliza-se de processos criptográficos baseados tanto em chaves assimétricas como com chaves simétricas.

A recomendação atual da EMV é a utilização do RSA como algoritmo de chave públicas (chaves de até 2048 bits e expoente 2^16+1) e 3DES (com chaves de 112 bits).

Portanto hoje em um cartão devem existir as seguinte chaves :

- Chave privadas/ públicas :
    - Chave pública do emissor – utilizada nos processos de autenticação do cartão SDA/DDA , criptografia de pin offline.
    - Chave pública do cartão (no caso da autenticação dinâmica) - utilizada nos processos de autenticação do cartão SDA/DDA, , criptografia de pin offline.
- Chave simétricas:
    - Master Key do cartão – derivada a partir da chave master do emissor, utilizada nos processos de autenticação da transação e validação da autenticação do emissor.

3.2.1. Autenticação do cartão

Existem dois mecanismos de autenticação dos dados presentes em um cartão EMV [1] :

- SDA – Static Data Authentication - Baseado em uma assinatura digital estática dos dados do cartões utilizando um mecanismo de chaves públicas
- DDA – Dynamic Data Authentication – Baseado em uma assinatura digital dinâmica dos dados do cartões utilizando um mecanismo de chaves públicas

Estes mecanismos são importantes para manter a integridade dos dados gravados em um cartão EMV, desta forma garante-se que os dados não foram adulterados.

3.2.1.1. Static Data Authentication

Na autenticação estática dos dados, um conjunto de dados do cartão são autenticados através de uma assinatura digital realizada pela chave pública do emissor do cartão.

Para que durante a realização desta verificação são necessário os seguintes componentes :

- Dados do cartão
- Assinatura digital
- Chave pública do emissor
- Certificado da chave pública do emissor emitido pela autoridade certificadora (CA)
- Chaves públicas da CA.

De posse destes dados é possível para o ATM ou terminal ou estação do banco realize a validação dos dados do cartão .

Uma característica importante deste mecanismo é que o único componente conhecido e confiável, para o terminal que estará autenticando o cartão, são as chaves públicas da CA, todos os demais dados são fornecidos pelo cartão.

Como podemos ver na figura abaixo o emissor autentica os dados do cartão com sua chave privada e envia um certificado da sua chave pública, o terminal por sua vez possue as chaves públicas da CA, que serão utilizadas para validar o certificado presente no cartão.

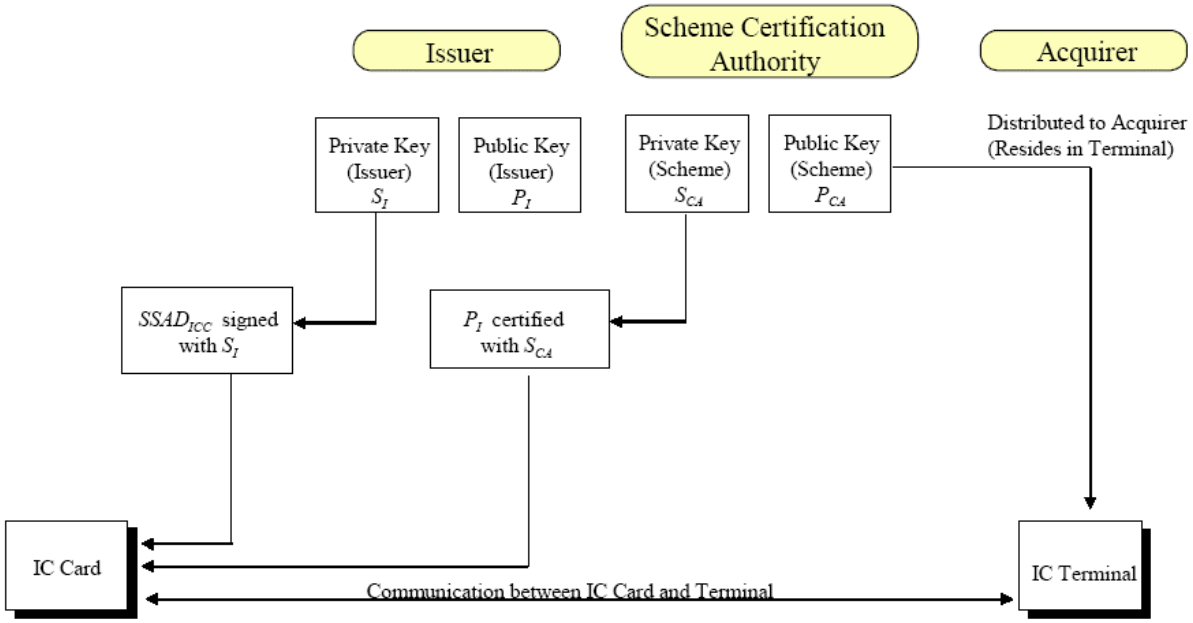

Fig 4 Esquema do SDA [1]

O certificado presente no cartão possue as seguintes informações:

Field Name	Length	Description	Format
Recovered Data Header	1	Hex. value '6A'	b
Certificate Format	1	Hex. value '02'	b
Issuer Identification Number	4	Leftmost 3-8 digits from the PAN (padded to the right with hex. 'F's)	cn 8
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary number unique to this certificate assigned by the certification authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme[11]	b
Issuer Public Key Algorithm Indicator	1	Identifies the digital signature algorithm to be used with the Issuer Public Key[11]	b
Issuer Public Key Length	1	Identifies the length of the Issuer Public Key Modulus in bytes	b
Issuer Public Key Exponent Length	1	Identifies the length of the Issuer Public Key Exponent in bytes	b
Issuer Public Key or Leftmost Digits of the Issuer Public Key	N_{CA} – 36	If $N_I \leq N_{CA} - 36$, this field consists of the full Issuer Public Key padded to the right with $N_{CA} - 36 - N_I$ bytes of value 'BB' If $N_I > N_{CA} - 36$, this field consists of the $N_{CA} - 36$ most significant bytes of the Issuer Public Key[12]	b
Hash Result	20	Hash of the Issuer Public Key and its related information	b
Recovered Data Trailer	1	Hex. value 'BC'	b

Fig.5 Dados presentes no certificado da chave pública do emissor[1]

Como todo certificado digital , temos armazenado no cartão campos como : validade, identificação do certificado, algoritmo utilizado, identificação do emissor.

Abaixo temos o algoritmo de autenticação estática :

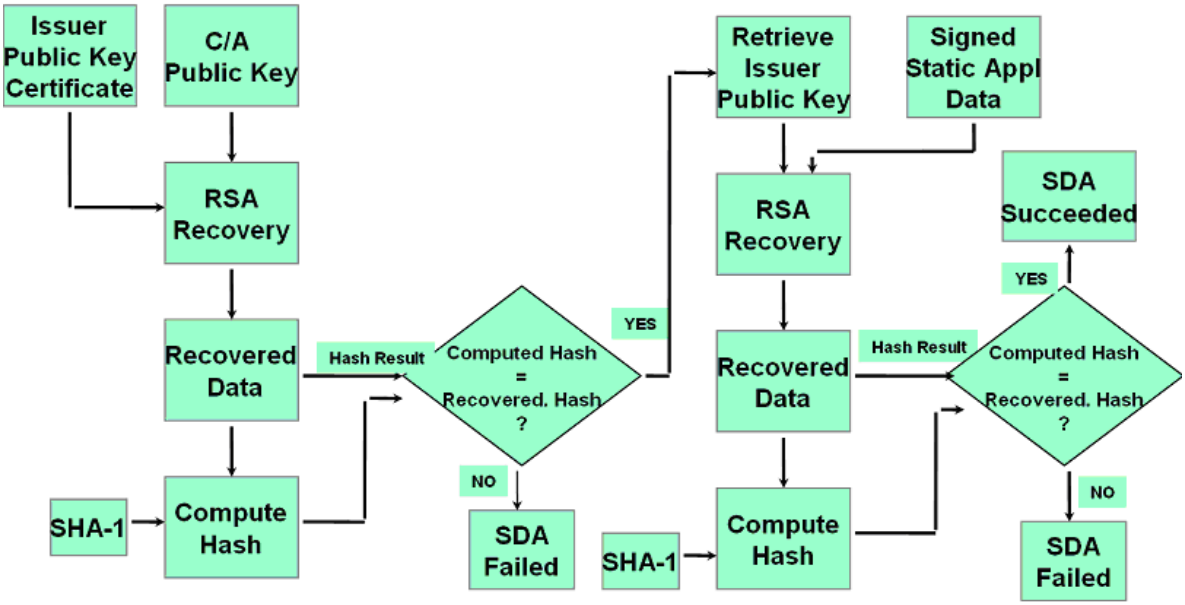

Fig 6 Algoritmo de validação do SDA em um cartão EMV.

Este é o mecanismo mais utilizado atualmente na autenticação de cartões, isso se deve ao fato de não requerer que o cartão seja capaz de processar criptografia RSA, uma vez que a assinatura é realizada em cima de dados estáticos do cartão. Outra vantagem deste método é que o emissor não é obrigado a gerar e administrar um conjunto de chaves públicas/ privadas para todos os cartões, sendo que com apenas uma única ele pode autenticar todos os cartões.

Por outro lado temos como desvantagem a possibilidade de realizar cópias dos cartões (ainda que somente dos dados do cartão, não das chaves de autenticação) desde que não sejam alterados os dados do cartão.

3.2.1.2. Dynamic Data Authentication

Na autenticação dinâmica dos dados, um conjunto de dados do cartão são autenticados através de uma assinatura digital processada dinamicamente pelo cartão. Neste caso é necessário que o cartão possua a capacidade de processar RSA ou o algoritmo de chaves públicas indicado pelo cartão.

A DDA requer quase os mesmo componentes para a autenticação:

- Dados do cartão
- Assinatura digital
- Chave pública do emissor
- Certificado da chave pública do emissor emitido pela autoridade certificadora (CA)
- Chave pública do cartão
- Certificado da chave pública do cartão emitido pelo emissor
- Chaves públicas da CA.

De posse destes dados é possível para o ATM ou terminal ou estação do banco realize a validação dos dados do cartão .

Uma característica importante deste mecanismo é que o único componente conhecido e confiável, para o terminal que estará autenticando o cartão, são as chaves públicas da CA, todos os demais dados são fornecidos pelo cartão.

O processo inicial é parecido com a DAS, no cartão existe a chave pública do emissor juntamente com o certificado da CA, além disso também está presente no cartão a chave pública do cartão e o certificado da chave pública do cartão assinado pelo emissor.

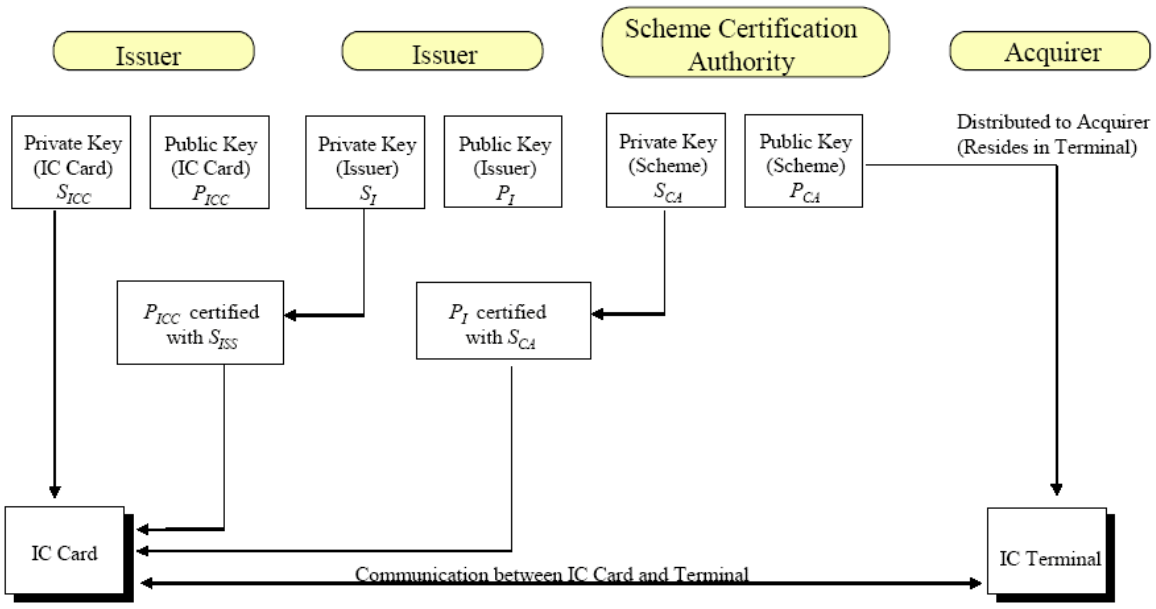

Fig.7 Diagrama da DDA [1]

A validação da chave pública do emissor é realizada como demonstrado no SDA.

Como na autenticação SDA, os certificados possuem todas as informações necessárias, para identificá-los, abaixo podemos ver os dados constantes no certificado da chave pública do cartão :

Field Name	Length	Description	Format
Certificate Format	1	Hex. value '04'	b
Application PAN	10	PAN (padded to the right with hex. 'F's)	cn 20
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary number unique to this certificate assigned by the issuer	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme[11]	b
ICC Public Key Algorithm Indicator	1	Identifies the digital signature algorithm to be used with the ICC Public Key[11]	b
ICC Public Key Length	1	Identifies the length of the ICC Public Key Modulus in bytes	b
ICC Public Key Exponent Length	1	Identifies the length of the ICC Public Key Exponent in bytes	b
ICC Public Key or Leftmost Digits of the ICC Public Key	$N_I - 42$	If $N_{IC} \leq N_I - 42$, this field consists of the full ICC Public Key padded to the right with $N_I - 42 - N_{IC}$ bytes of value 'BB' If $N_{IC} > N_I - 42$, this field consists of the $N_I - 42$ most significant bytes of the ICC Public Key [15]	b
ICC Public Key Remainder	0 or $N_{IC} - N_I + 42$	This field is only present if $N_{IC} > N_I - 42$ and consists of the $N_I - N_{CA} + 42$ least significant bytes of the ICC Public Key	b
ICC Public Key Exponent	1 or 3	ICC Public Key Exponent equal to 2, 3 or $2^{16} + 1$	b
Static Data to be Authenticated	var.	Static data to be authenticated as specified in the *ICC Application Specification for Payment Systems*	b

Fig.8 Dados presentes no certificado da chave pública do cartão

Uma vez recuperado e validado todas as chaves e certificados presentes no cartão, a chave pública do cartão é utilizada para realizar a validação de uma assinatura gerada dinamicamente pelo cartão.

Abaixo temos o algoritmo DDA:

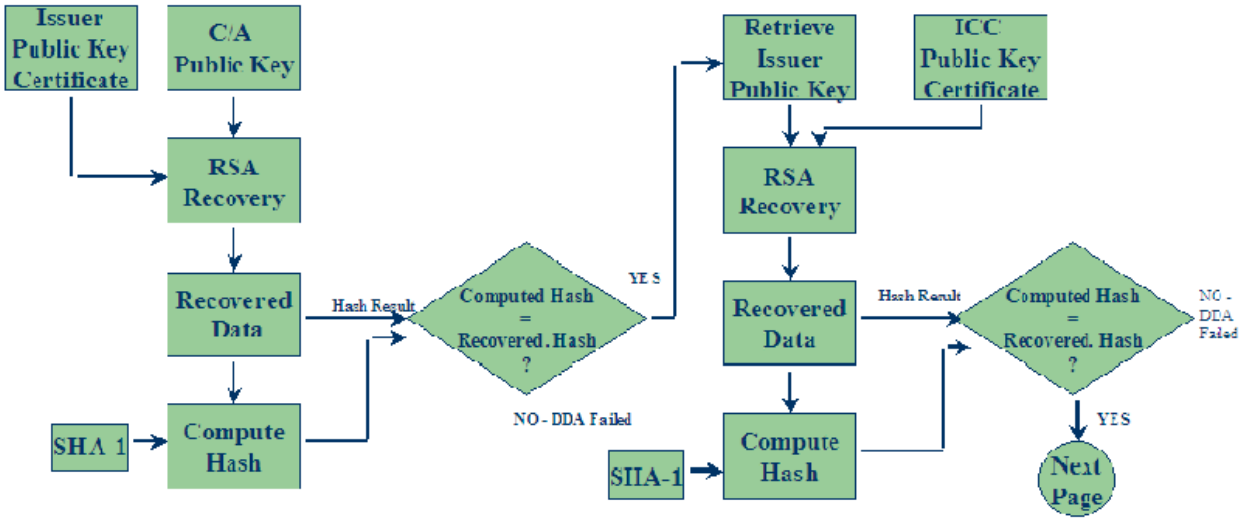

Fig.9 Algoritmo DDA – Parte 1

O terminal pede ao cartão que gere dinamicamente uma assinatura dos dados do cartão .

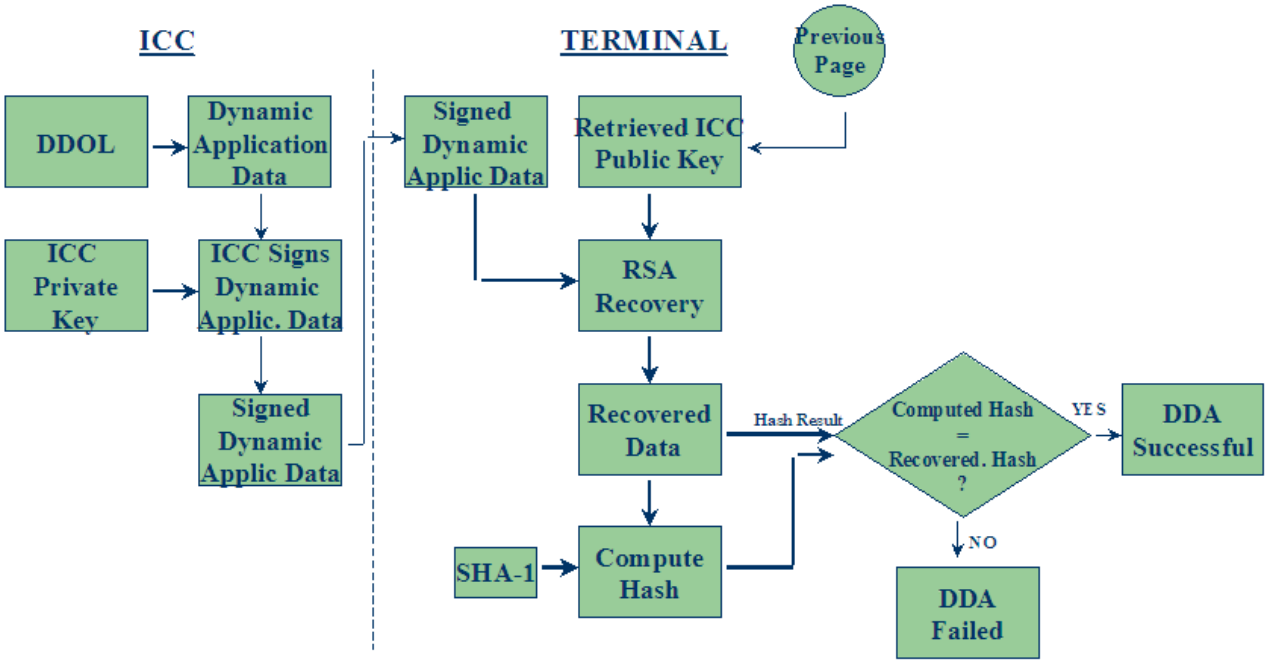

Fig.10 Algoritmo DDA – Parte 2

Apesar deste método ser mais seguro que o SDA, ele necessita que os cartões sejam capazes de processar RSA, e além disso o emissor deverá gerar conjuntos de chaves públicas e privadas para cada cartão.

3.2.2. Autenticação do usuário

Dentro do cartão também estará definido o método de autenticação do portador do cartão, este método poderá variar de acordo com o valor da transação e capacidade do terminal que processa a mesma.

Os principais mecanismos de autenticação são :

- Senha offline – Na senha offline, a senha é capturada por algum dispositivo de captura de pin e enviada em claro para a validação do cartão.
- Assinatura – este método é o mesmo que o de cartões magnéticos, e baseia-se na verificação visual da assinatura do portador.
- Senha Online – a senha é capturada e criptografada para ser validada online pelo emissor do cartão.
- Senha offline criptografada – a senha é capturada por algum dispositivo de captura de pin e enviada criptografada pela chave pública do cartão e validada pelo cartão, de acordo com o algoritmo demonstrado abaixo .

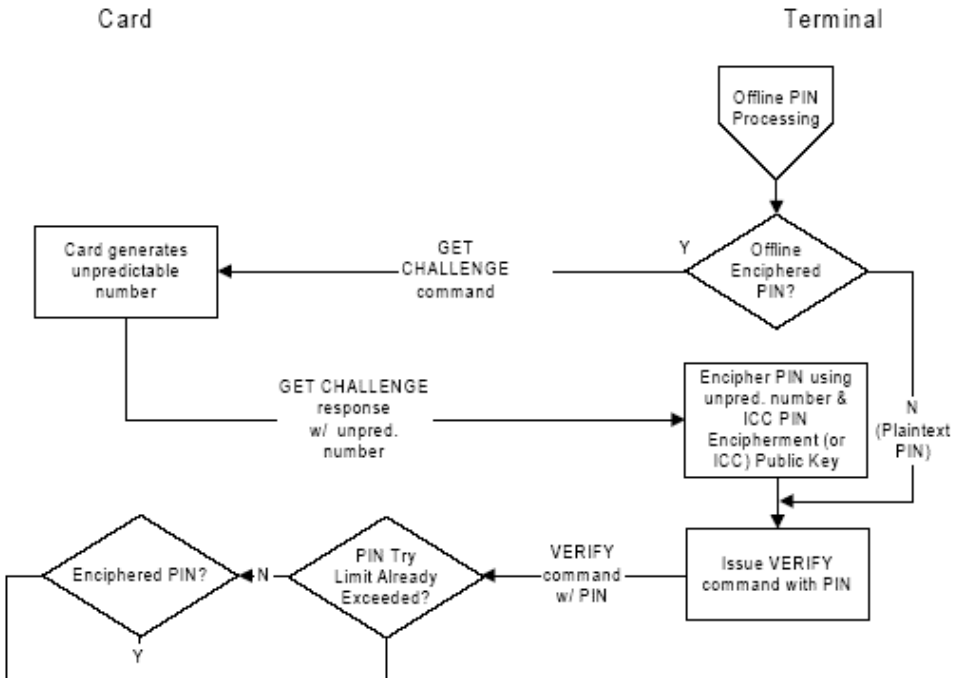

Fig.11 Pin offline criptografado

Vantagens / desvantagens do métodos :

Método	Vantagem	Desvantagem
Senha offline	Autenticada localmente pelo cartão, possibilitando a realização de transações offlines com maior segurança	Como a senha é enviada em claro ao cartão, seria possível interceptar a comunicação entre o leitor e o cartão e conseqüentemente ter acesso à senha
Senha online	Mesmo procedimento utilizado atualmente em muitas transações com cartão de crédito/ débito	Requer uma conexão online com o emissor do cartão para a validação da senha.
Assinatura	Não requer quase nenhuma capacidade adicional no terminal que processa a transação.	Baixa segurança, depende do operador do terminal para o sucesso da validação
Senha criptografada offline	Idem à senha offline	Requer que o cartão seja capaz de processar RSA.

3.2.3. Autenticação da transação

Após a devida validação do cartão, e do portador do cartão, um dos pontos mais importantes é a autenticação da transação.

Todas as transações realizadas por um cartão EMV devem estar devidamente autenticadas através de um MAC (message Authentication Code).

A utilização de MACs nas transações garantem:

- Integridade da transação – os dados não foram maliciosamente alterados
- Não repúdio – a transação foi realizada na presença do cartão.

O processo de autenticação sugerido pela norma se baseia na utilização de chaves simétricas 3DES.

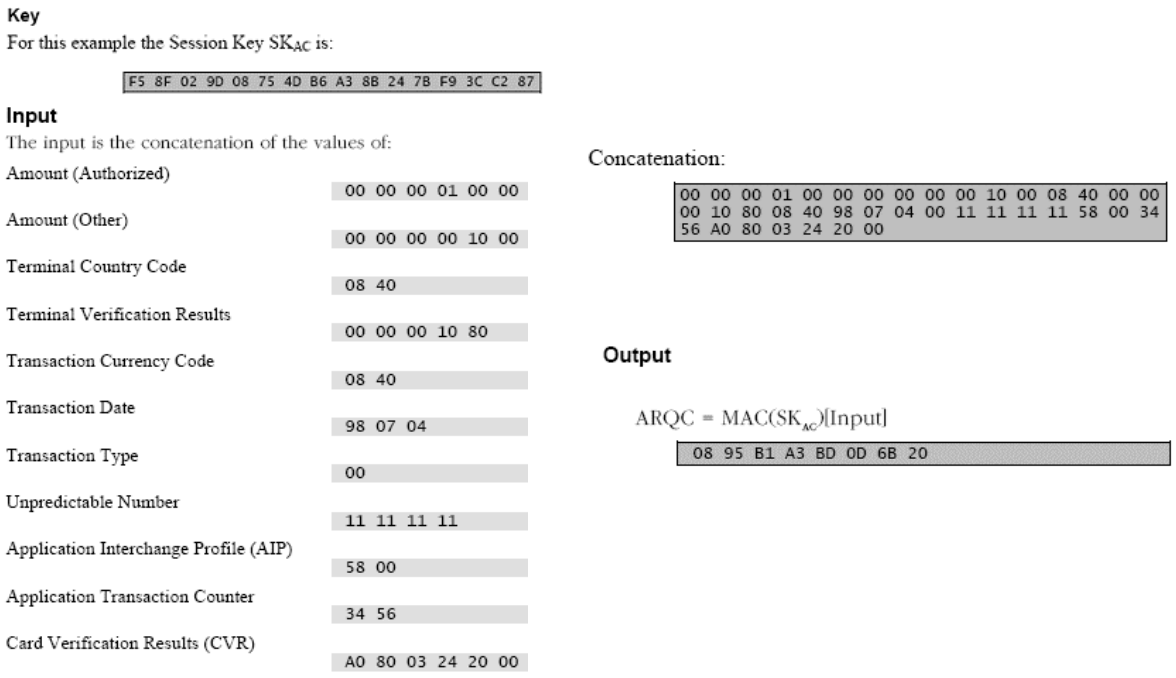

Fig.12 Exemplo autenticação de uma transação

O exemplo acima foi realizado utilizando uma chave de sessão simétrica que é gerada a partir da diversificação de uma chave do cartão.

Um ponto importante no processo é que a chave master do cartão nunca é utilizada sem diversificação, de forma a evitar replay attacks, em geral a chave é sempre diversificada ou por um número imprevisível ou mais comumente pelo contador de transações do cartão.

Figure B–1: MAC Algorithm for Double-Length DEA Key

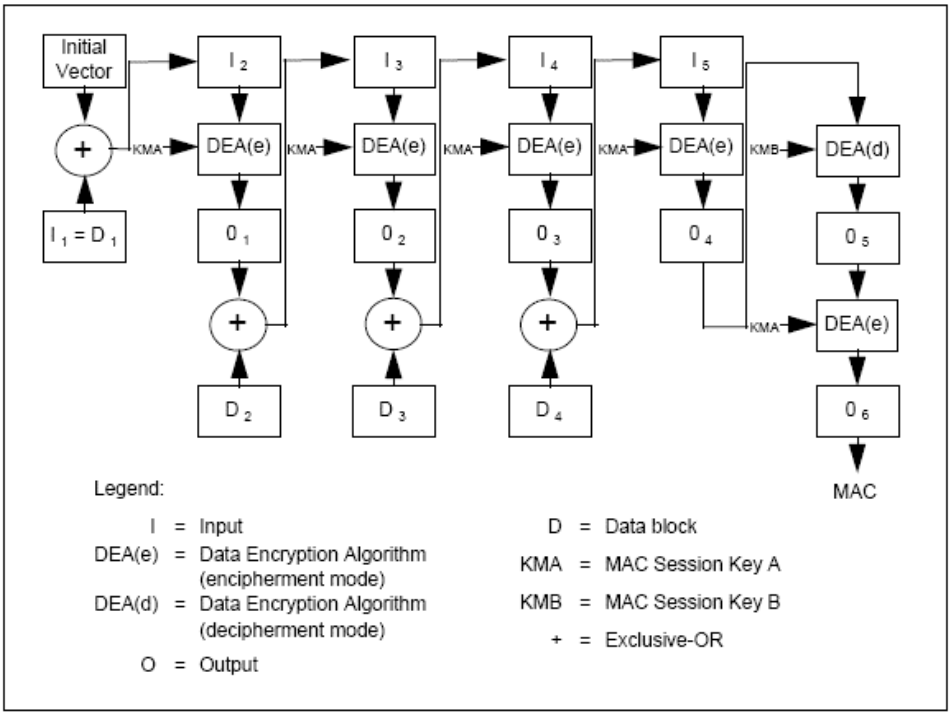

Fig.13 Algoritmo de geração de MAC

3.2.4. Autenticação do banco

Após a execução de uma transação online, o banco deve aprovar a operação, autenticando o código de resposta com a chave Master do cartão.

Este protocolo garante que durante uma comunicação com o emissor, um hacker intercepte uma comunicação e modifique os códigos de autorização do emissor.

Abaixo temos um exemplo de autenticação da reposta de um emissor o ARPC (Authorisation Response Cryptogram).

ARPC Generation

Key

The Card Master Key MK_{AC} for ARPC generation is the same key used for AC computation and validation as shown above:

```
08 DF 34 25 32 20 A7 20 EF F2 C1 34 38 52 E6 3D
```

Input

The input is the XOR of:

The Authorization Response Code (ARC) (right-padded with zero bytes)

```
31 30
```

The ARQC

```
08 95 B1 A3 BD 0D 6B 20
```

The XOR (ARC || 0 0 0 0 0 0) ⊕ ARQC:

```
39 A5 B1 A3 BD 0D 6B 20
```

Output

$$ARPC = DES3(SK_{AC})[Input]$$

```
4C F0 35 9C 80 0E 13 C2
```

Fig. 14 Exemplo Autenticação Emissor

3.3. Evolução

Os algoritmos descritos acima são os definidos na versão 3.1.1 da norma EMV, esta versão foi criada em 1996 e somente agora está sendo implementada em grande escala, no entanto em 2000, foi lançado uma nova versão EMV 4.0 que é compatível com a EMV 3.1.1.

A maior mudança em termos de segurança na nova versão, foi a introdução de um mecanismo de autenticação de cartão e transação combinado que se baseia em um algoritmo de chaves públicas, este mecanismo foi definido como CDA, Combined Dynamic Data Authentication [8].

Outro mecanismo intressante definido tanto na norma EMV 4.0 [9] como na EMV 3.1.1 [4] , é a utilização do cartão EMV em transações de comércio eletrônico. A figura abaixo mostra como seria o desenho de um sistema com EMV + SET .

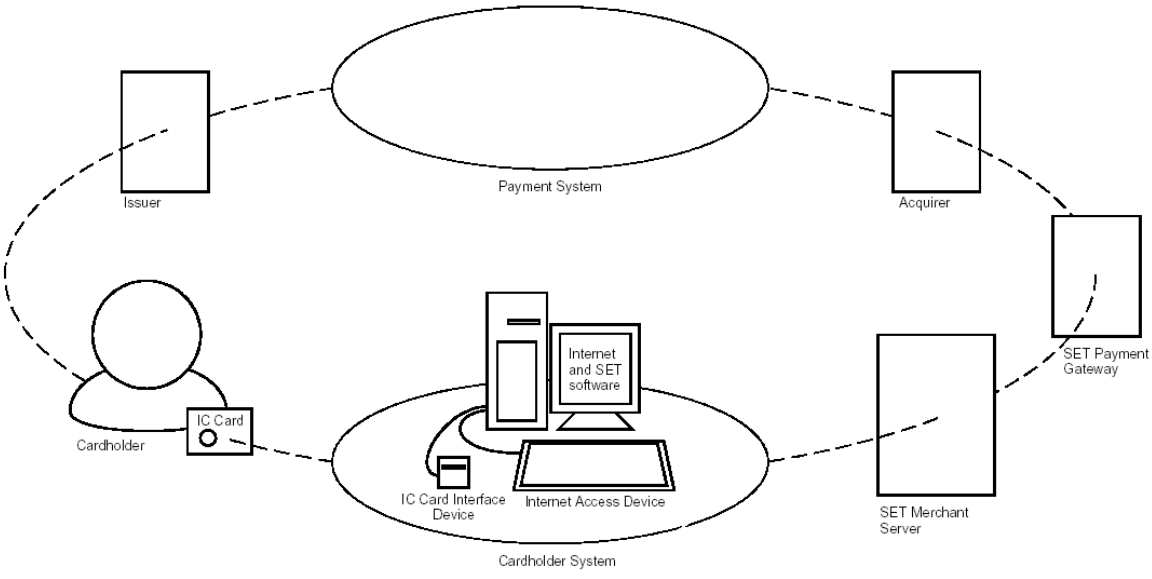

Fig. 15 Sistema SET com cartões EMV

Nesta configuração, o cartão seria responsável por gerar criptogramas com os quais o emissor poderia autenticar o cartão, processar e validar opcionalmente a senha do cartão de modo offline e até mesmo o certificado do portador do cartão poderia estar disponível dentro do cartão .

Abaixo temos em linhas gerais como seria uma transação utilizando um cartão EMV + SET :

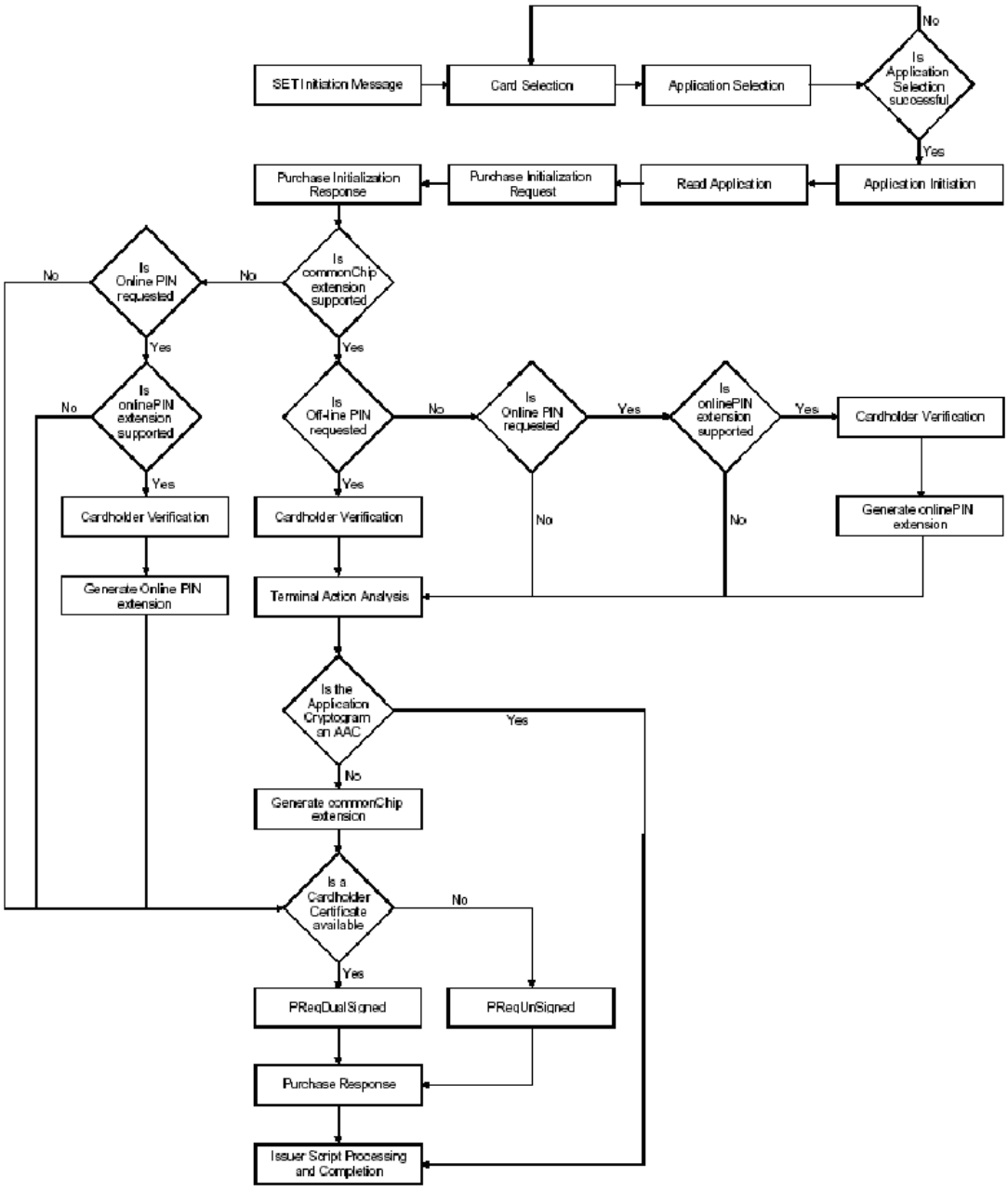

Fig.16 Diagrama do fluxo de uma transação SET + EMV [9]

Ainda como evolução da EMV ainda poderemos ter :

- Novos métodos de autenticação de usuário , baseados em biometria (impressão digital, íris, etc...) [11]
- Substituição dos Algoritmos de criptografia simétricos utilizados nas autenticações da transação e emissor por algoritmos mais seguros e poderosos como os de chave públicas [8].
- Outros algoritmos poderão substituir o RSA (utilizado na autenticação dos cartões) por outros como o de curvas elípticas [10].

4. Conclusão

O uso de SmartCards provê um aumento significativo no nível de segurança das transações de pagamentos com cartões de crédito, pelo uso de certificados digitais, assinaturas digitais e criptografia de chave pública e simétrica, utilizando técnicas similares às empregadas em comércio eletrônico usando infraestrutura Web.

A norma EMV procura conciliar os requisitos de segurança com custos na emissão e gerenciamento dos cartões e chaves associadas, num compromisso entre minimizar o risco das transações e não elevar excessivamente os custos de emissão e gerenciamento dos cartões e chaves associadas, uma vez que os cartões de crédito são produtos distribuidos em larga escala.

5. Referências

[1] – EMV ’96 – Integrated Circuit Card – Specification for Payment Systems – Version 3.1.1 - www.emvco.com

[2] – EMV ’96 – Integrated Circuit Card Application – Specification for Payment Systems – Version 3.1.1 - www.emvco.com

[3] – EMV ’96 – Integrated Circuit Card Terminal – Specification for Payment Systems – Version 3.1.1 - www.emvco.com

[4] – EMV ’96 – Chip Electronic Commerce Specification – Version 1.0 - www.emvco.com

[5] – EMV – Issue and Application Security Guidelines – Version 1.2 –

[6] – IBM – SmartCards : A case Study – Jorge Ferrari , Robert Mackinnon, Susan Poh, Lakshman Yatawara – www.redbooks.ibm.com

[7] – EMV – Application Independent ICC to terminal Interface Requirements – Version 4.0 - www.emvco.com

[8] – EMV – Security and key Management – Version 4.0 – www.emvco.com

[9] – EMV – Application Specification – Version 4.0 – www.emvco.com

[10] – EMV Elliptic Curve – Technical Report – Version 1.0 – www.emvco.com

[11] – Visa Integrated Circuit Card – Application Overview – Version 1.4.0 – international.visa.com