MODELO GLOBAL

Versão 5.02

LIVRO II

CAPÍTULO D
SERVIÇO NA INTERNET

D.1 SERVIÇO MBNet

D.2 SERVIÇOS DE ACESSO AO MULTIBANCO

D.3. AUTENTICAÇÃO FORTE

D.1 SERVIÇO MBNet

O MBNet é um serviço prestado por entidades intervenientes no sistema de pagamentos português (Bancos Aderentes, SIBS e Unicre), que permite a realização de operações de autorização e de liquidação de compras na Internet, com garantias acrescidas de segurança para os clientes e comerciantes *online*. Indicam-se em seguida as entidades intervenientes no serviço.

D.1.1 INTERVENIENTES NO SERVIÇO MBNet

D.1.1.1 CLIENTE

Indivíduo com acesso à Internet (loja virtual) que pretende efectuar pagamentos. Para tal, necessita de ser titular de um cartão emitido por uma instituição participante no sistema e ter aderido ao serviço MBNet. A adesão ao serviço pode ser efectuada ou utilizando os Caixas Automáticos da Rede Multibanco (CAs) através da operação serviço MBNet, ou directamente junto do Emissor.

D.1.1.2 EMISSOR

Entidade que disponibiliza aos seus clientes o acesso ao MBNet, podendo efectuá-lo através de canais de distribuição próprios (ex.: Banca Telefónica, *Home Banking*) ou através da rede de CAs Multibanco. No caso de pretender utilizar canais internos, deverá implementar mensagens *real-time* com a SIBS (ver capítulo **D.4** - Livro III), ou utilizar o **Terminal de Serviços SIBS**.

Para o processamento das operações efectuadas pelos seus clientes, utilizando este canal de pagamento, o Emissor deve implementar o tratamento das operações definidas no ficheiro **Destinos** (MDST5) e capítulo **D.3.2** do Livro III.

À semelhança das restantes operações efectuadas no Sistema Multibanco, o Emissor do cartão deve enviar à SIBS a **Caracterização do BIN** e a **Caracterização do CPD** devidamente preeenchidas, caso pretenda possibilitar aos titulares dos cartões por si emitidos, a utilização deste canal de pagamento.

Para que os seus clientes possam efectuar pagamentos seguros em comerciantes não aderentes, utilizando cartões temporários, o Emissor terá que solicitar um novo BIN ao sistema de pagamentos correspondente aos cartões em causa (MasterCard ou Visa), que será utilizado pela SIBS unicamente para a geração deste tipo de cartões, e preencher a **Caracterização do BIN Temporário**.

D.1.1.3 COMERCIANTE ADERENTE

Entidade que possui um *site* na Internet ("loja virtual") e pretende proporcionar aos titulares de cartões nacionais a opção de Pagamento MBNet. Para aderir ao serviço MBNet deve contactar com o Representante, para a celebração de um contrato de adesão a este novo serviço. Deve ainda implementar o serviço de acordo com as especificações definidas pelo sistema de pagamentos nacional.

O comerciante, ao exprimir a sua intenção de aderir ao serviço, deve receber um documento explicativo do processo de adesão, com a indicação dos requisitos mínimos necessários à sua implementação. Após a assinatura do contrato com o Representante, será disponibilizada documentação, com as especificações técnicas do serviço, a definição e calendarização da certificação e a indicação dos serviços de apoio.

D.1.1.4 REPRESENTANTE - UNICRE

Entidade responsável pela contratação do comerciante no processo de adesão ao serviço MBNet. A Unicre tem também a responsabilidade de registar o comerciante no Sistema Multibanco via Terminal de Serviços SIBS, bem como de solicitar a emissão de um certificado digital para o Terminal de Pagamento Automático Virtual.

Actualmente, a solicitação de emissão deste certificado digital é feita junto da Autoridade de Certificação MULTICERT.

D.1.1.5 SIBS

Entidade encarregue da gestão técnica e operacional do serviço, garantindo a integridade e segurança dos dados transmitidos entre todos os intervenientes no processo. Atribui de forma automática a Identificação MBNet ao Cliente, garantindo a sua integridade e unicidade no sistema.

Disponibiliza ao Representante a possibilidade de inserir comerciantes, estabelecimentos e TPAs virtuais através da utilização do Terminal de Serviços SIBS.
Atribui de forma automática, o(s) número(s) de TPA Virtual solicitado(s) para o comerciante aderente, garantindo a sua unicidade no sistema de pagamentos.
Disponibiliza aos Emissores (Bancos e Unicre) a possibilidade de efectuarem um conjunto de operações no serviço MBNet - adesão, consultas, alterações, *resets* e cancelamento de cartões - utilizando o Terminal de Serviços SIBS e/ou as mensagens *Host-to-Host*.

D.1.1.6 VISA, *3-D SECURE*

O protocolo *3-D Secure* é um sistema da Visa que pretende acrescentar segurança na validação dos pagamentos efectuados na Internet. O *3-D Secure* é uma tecnologia de autenticação que usa encriptação SSL (*Secure Sockets Layer*) e um *Merchant Server Plug-in* para:

- Enviar informação e solicitar aos participantes a autenticação do cliente quando este efectuar uma compra *online*, e
- Proteger a informação, do cartão utilizado na compra, transmitida via Internet.

A denominação 3-D tem origem no modelo de repartição das entidades e funções, por estas assumidas, em três domínios.

Domínio do *Issuer*

O *Issuer* é responsável por:

- gerir a adesão dos seus clientes ao serviço (incluindo a verificação de identidade do cliente) e a autenticação dos mesmos nas operações de pagamento via Internet.

Domínio do *Acquirer*

O *Acquirer* é responsável por:

- definir os procedimentos que asseguram que os comerciantes participantes em transacções Internet estão a operar sob um *merchant agreement* com o *Acquirer*, e
- disponibilizar a infra-estrutura de processamento para as transacções de autenticação.

Domínio de Interoperabilidade

Este domínio consiste, lato senso, na Internet, isto é, um conjunto de protocolos comuns e serviços partilhados que permite facilitar a troca de transacções (autenticação e pagamento) entre os dois domínios anteriores.
Para mais detalhe sobre o *3-D Secure* pode ser consultado o site **http://international.visa.com**.

D.1.1.6.1 IMPLEMENTAÇÃO DO 3-D SECURE NO MBNet

A solução para a implementação do *3-D Secure* no MBNet compreende as duas fases do serviço: a Adesão e a Autenticação.

Adesão ao Serviço MBNet *3-D Secure*

A Visa não impõe uma solução *standard* para o processo de adesão ao serviço. Compete ao Emissor implementar uma solução que:

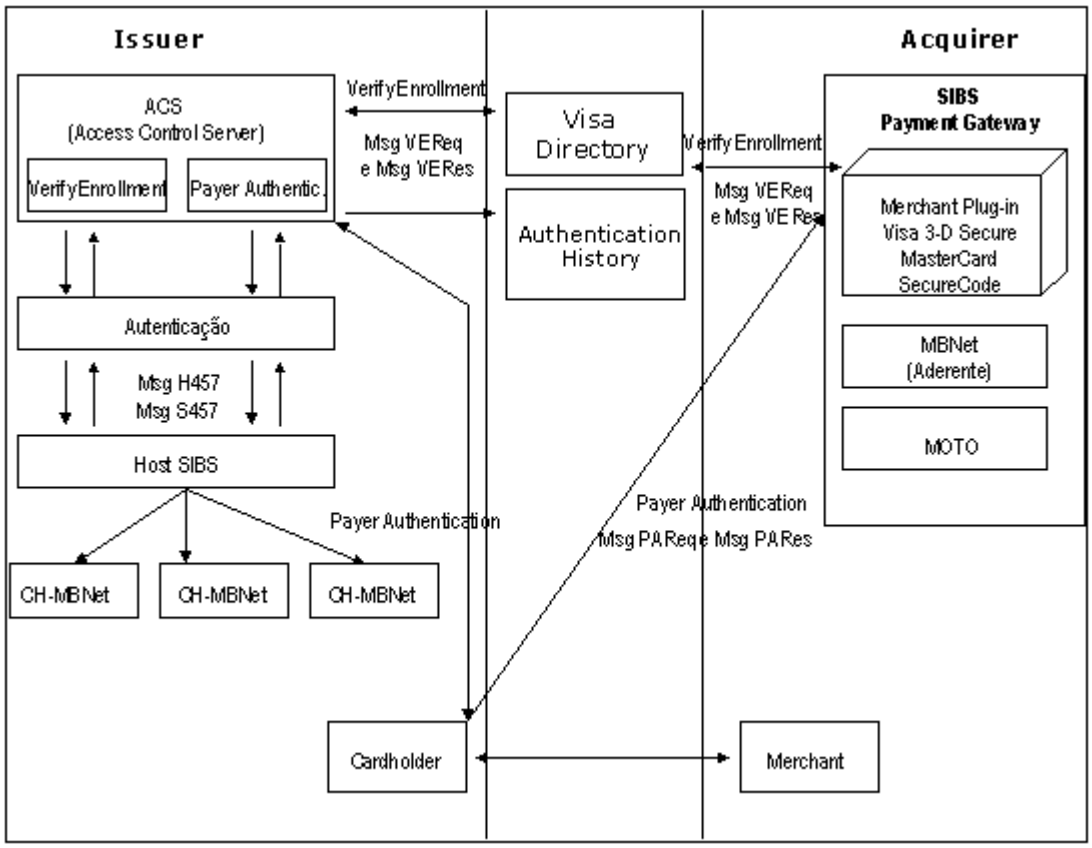
- solicite ao cliente dados do seu cartão, passwords e/ou segredos partilhados,
- disponha de um Servidor de Adesões (*Enrollment Server*), para gerir este processo,
- disponha de um Servidor de Controlo de Acessos (*Access Control Server*), para que em cada operação de autenticação se possa verificar que de facto o cliente está registado no serviço,

assegurando a correcta identificação do cliente durante o processo de adesão.

O processo de Adesão ao MBNet satisfaz estes requisitos.

Autenticação MBNet *3-D Secure*

A solução para o processo de Autenticação de uma transacção MBNet *3-D Secure* é ilustrada na seguinte figura.



SIBS PAYMENT GATEWAY - VISA *3D-SECURE*

D.1.1.6.2 PROCESSOS IMPLEMENTADOS PELA SIBS

A SIBS obteve a certificação Visa do seu *Merchant Server Plug-in* (MPI) versão 1.0.2 do Protocolo *3-D Secure* e versão 2.9 MBNet em 1 de Abril 2003. A certificação Visa do *Access Control Server* (ACS) versão 1.0.2 do Protocolo *3-D Secure* e versão 2.9 MBNet foi obtida em 15 de Dezembro 2003.

D.1.1.6.3 ADESÃO DOS EMISSORES AO VERIFIED BY VISA (3-D SECURE)

Os emissores que participem no MBNet e que pretendam aderir ao VbV devem contactar a Visa Europa solicitando a sua adesão a este serviço. Dado que a SIBS desenvolveu o *Access Control Server* os emissores têm unicamente de efectuar o seguinte:

- Carregamento dos BINs e cartões no VbV.
- Obtenção dos certificados digitais para o serviço.
- Emissão de uma *Authorisation Letter* para informar a VISA que a SIBS é a entidade que processará os certificados digitais e as chaves privadas do Emissor.

Para cada uma destas acções existem formulários próprios que são fornecidos aos emissores pela Visa Europa.

D.1.2 COMPONENTES DO SERVIÇO

A matriz seguinte apresenta as diversas componentes do serviço.

MBNet - Quadro Resumo

O QUÊ? / QUEM?	**REGISTO** (Inscrição, Alteração, Cancelamento)	**OPERAÇÃO** (Autorização MBNet, Cancelamento autorização MBNet, Compra após autorização, Devolução)
CLIENTE	Na Rede MB-CA - Operação de Serviço Especial Junto do Emissor - A definir pelo Emissor	- Se Comerciante registado -> introdução de Identificação e Código Secreto para pedido de validação - Se Comerciante não registado -> introdução de Identificação e Código Secreto para pedido de número de cartão temporário
EMISSOR	Na Rede MB-CA - Caracterização de BINs / CPD - Mensagens *Real-Time* (opcional) - Registo Ficheiro **Destinos** (MDST5) Junto do Emissor - Mensagens *Real-Time* - Utilização Terminal de Serviços SIBS	- Códigos de transacção MBNet - Mensagens para Autorização MBNet, Cancelamento autorização MBNet, Compra após autorização, Devolução - Códigos de transacção no Ficheiro **Destinos** (MDST5) - Pedido de BIN (Visa / MasterCard / AMEX) para cartões temporários - Gestão de cativos em contas D.O.
COMERCIANTE	Contrato com o *Acquirer* (Unicre / AMEX)	- Implementação das especificações técnicas (operações TPA) - Certificados - Certificação
ACQUIRER (UNICRE)	Inscrição de Comerciantes, Estabelecimentos virtuais, TPAs virtuais e condições contratuais (via Terminal de Serviços SIBS)	- Códigos de transacção nas mensagens *Real-Time* - Códigos de transacção no ficheiro de movimentos
SIBS	Em acréscimo ao referido acima, nomeadamente: - Gestão da Base de Dados de aderentes ao MBNet - Disponibilização de mensagens a trocar entre o servidor MBNet e o *Host* - Gestão dos cartões temporários	

D.1.3 REGISTO

No serviço MBNet existem dois registos em função do tipo de aderente:

- **Registo do cliente**
  O cliente de uma das instituições emissoras de cartões aderentes ao MBNet e possuidor de um cartão reconhecido na rede de terminais MB, pode aderir ao serviço MBNet, utilizando os Caixas Automáticos da Rede Multibanco ou através de canais próprios disponibilizados pelo seu Emissor.

- **Registo do comerciante** (que é efectuado junto do Representante)
  É da responsabilidade do Representante efectuar o registo do comerciante aderente, através do Terminal de Serviços SIBS, no serviço Gestão de Pagamento Automático.
  Ao matricular o comerciante no Sistema MB, e no caso deste ainda não existir, o Representante deve inserir um novo estabelecimento do tipo Virtual, no qual só pode matricular terminais de pagamento automático (TPAs) virtuais, e deve pedir a produção de cartões de supervisor em euros para o TPA Virtual.
  Os Representantes devem inserir os seus acordos de representação.
  A descrição detalhada do impacto técnico para o Representante Unicre, encontra-se descrita no documento "MBNet - Documento Técnico - Interface Unicre".

D.1.3.1 REGISTO DO CLIENTE NO SERVIÇO ESPECIAL DOS CAs MB

O serviço especial MBNet é disponibilizado nos CAs da Rede MB, aos clientes possuidores de cartões aceites na rede e cujos Emissores o autorizem.

Na opção de Serviço MBNet, o Cliente tem ao seu dispor as seguintes operações:

- Adesão ao serviço
- Alteração do Código Secreto MBNet
- Alteração do montante máximo de compras por dia
- Pedido de 2ª via de talão
- Cancelamento do serviço

D.1.3.2 REGISTO DO CLIENTE NOS CANAIS PRÓPRIOS DO EMISSOR

Sempre que o Emissor pretenda utilizar canais próprios de adesão (banca telefónica, *home banking*, etc.), deve implementar um conjunto de mensagens que são posteriormente trocadas entre o *Host* do Emissor e o da SIBS, designadas por mensagens *Host-to-Host*. Paralelamente e como *backup*, a SIBS também disponibiliza estas funções no Terminal de Serviços SIBS.

A SIBS recomenda preferencialmente a utilização de mensagens *Host-to-Host*, devendo ficar reservada a utilização do Terminal de Serviços SIBS para situações de excepção.

D.1.3.2.1 MENSAGENS HOST-TO-HOST DO SERVIÇO MBNet

As mensagens *Host-to-Host* permitem ao Emissor, ter acesso em *real-time* à base de dados central de identificação dos seus cartões no serviço MBNet. Só após a correcta identificação, o cliente pode efectuar as operações disponíveis para este serviço: aderir, consultar, alterar e cancelar.

É de notar que o Código Secreto MBNet e a Identificação MBNet nunca estão presentes na mesma mensagem.

Nas sessões *real-time* entre os Emissores e a SIBS, a manutenção do contexto e a gestão de não respostas (ou respostas fora de tempo) é da responsabilidade do Emissor dos pedidos, no caso vertente, o Banco. Desta forma, quando o Banco não recebe uma resposta a um pedido enviado à SIBS, de facto não sabe se o pedido chegou ao seu destino e se, tendo sido entregue, terá sido respondido positiva ou negativamente. Não pode portanto ter uma certeza para indicar ao cliente.

Para obter essa certeza, o Emissor deve:

- classificar do seu lado estas mensagens como recuperáveis
- nos casos acima descritos assumir que a SIBS não recebeu o pedido
- indicar ao cliente que o pedido não foi processado
- esperar pela resposta da SIBS e enviar uma anulação

Os Emissores que pretendam implementar estas mensagens devem formalizar o seu pedido junto da SIBS.

Ver **Lista de Mensagens**.

D.1.3.2.2 TERMINAL DE SERVIÇOS SIBS

No Terminal de Serviços SIBS, as operações estão separadas em dois serviços: **Adesão ao Serviço MBNet** e **Gestão do Serviço MBNet**. Para que sejam reunidas as condições mínimas de confidencialidade, cada terminal só deve ter disponível um dos serviços referidos.

A operação de Adesão está disponível em MBNet Adesão; as restantes operações estão disponíveis em MBNet Gestão.

Os Emissores que pretendam utilizar o Terminal de Serviços SIBS devem indicar à SIBS, utilizando o impresso próprio, para que números de terminais pretendem os respectivos serviços de Adesão e Gestão MBNet.

D.1.3.2.3 EMISSOR

O Emissor terá sempre conhecimento, por ficheiro de fim de dia enviado pela SIBS, das operações de adesão, alteração, consulta e cancelamento efectuadas pelos seus clientes no serviço MBNet, quer tenham sido efectuadas através de um Caixa Automático ou directamente pelos canais do Emissor (mensagem *Host-to-Host* ou Terminal de Serviços SIBS).

A descrição detalhada do impacto técnico para os Emissores (Bancos e Unicre), encontra-se descrita no Modelo Global - Livro III - capítulo **D.4** e capítulo **E**.

Ficheiro Destinos para os Bancos
As operações de adesão, alteração, consulta e cancelamento efectuadas pelos seus clientes no serviço MBNet, são informadas ao Banco Emissor do cartão no ficheiro Destinos (MDST5), no **tipo de registo 1**, como um Serviço Especial Bancário.

Log
Por cada operação efectuada na Rede MB é realizada a escrita de um registo no ficheiro de *Log* da SIBS. Esse registo pode ser consultado pelo serviço de Gestão da Rede da SIBS ou via Terminal de Serviços SIBS.

D.1.4 OPERAÇÕES

No MBNet as operações são efectuadas por vontade expressa do cliente aderente, são validadas pelo comerciante e pelas aplicações do Serviço MBNet e processadas pela SIBS, pelo Emissor e pelo Representante.

CENÁRIOS DE UTILIZAÇÃO

A utilização do serviço MBNet está disponível em dois cenários:

- *Utilização do serviço MBNet em Comerciantes Aderentes*
  O cliente utiliza a sua Identificação MBNet e Código Secreto MBNet para se autenticar perante o sistema, que, em caso de aceitação, assegura a comunicação da validade da mesma ao comerciante.

- *Utilização do serviço MBNet em Comerciantes Não Aderentes*
  O cliente utiliza a sua Identificação MBNet e Código Secreto MBNet para solicitar um cartão temporário, cujos dados introduzirá no *site* do comerciante (podendo utilizar funções de *copy/paste*).

Com a integração do Sistema *3-D Secure* da Visa no MBNet, há que distinguir em cada um dos cenários, as operações efectuadas em comerciantes aderentes ou não a este sistema. Esta informação é fundamental na medida em que dela depende a possibilidade de se efectuarem repudiações de operações por incorrecta autenticação do cliente.

Assim:

- As operações efectuadas por um cliente MBNet num comerciante aderente ao MBNet, são informadas como operações MBNet independentemente do comerciante ser ou não aderente ao *3-D Secure* (o nível de segurança é o mesmo).
- As operações efectuadas com cartão real aderente ao *3-D Secure* num comerciante aderente ao *3-D Secure*, são informadas como operações *3-D Secure*.
- As operações efectuadas com cartão real não aderente ao *3-D Secure* num comerciante aderente ao *3-D Secure*, são informadas como operações MO/TO realizadas em comerciante seguro.

É também possível a utilização do cartão temporário (MBNet) em comerciantes não seguros (MO/TO). Estas operações são igualmente inequivocamente identificadas, como operações seguras ao nível da autenticação do cliente.

Ver **tabela de implementação**.

EMISSORES

Os Emissores aderentes ao serviço MBNet, devem indicar à SIBS quais os BINs cujos cartões têm acesso ao MBNet:

- No caso de BINs Visa, devem solicitar à Visa um BIN para a criação de cartões temporários;
- No caso de BINs MasterCard, devem solicitar à MasterCard um BIN para a criação de cartões temporários.

Devem indicar que estes BINs têm a SIBS como *processing center* na vertente *online* (pedidos de autorização).

Para os Emissores que pretendam ter mais do que uma entidade de *clearing*/*settlement* para o(s) BIN(s) de cartões temporários, têm que solicitar ao correspondente sistema de pagamento, tantos BINs quantas as entidades.

Posteriormente devem informar a SIBS dos BINs atribuídos, os quais são utilizados unicamente na criação de cartões temporários.

O serviço só está disponível para o Emissor, após a SIBS ter conhecimento da informação indicada no ponto anterior e a certificação técnica ter sido concluída com sucesso.

CLIENTES

Para utilizar o MBNet, o cliente necessita apenas de ter a possibilidade de aceder à Internet, ao *site* do comerciante para adquirir bens ou serviços e ao sistema MBNet para solicitar pedidos de autenticação (para efectuar pagamentos ou solicitar cartões temporários para utilizar em comerciantes não aderentes ao serviço).

Não é requerida a instalação de qualquer *hardware*, sendo opcional a instalação do ícone MBNet através de um pequeno *software* (4 kb) assinado digitalmente pela SIBS.

Tendo previamente efectuado a sua adesão, e após efectuar as encomendas no *site* do comerciante virtual, o cliente aderente deve aceder ao sistema MBNet e inserir a sua Identificação e Código Secreto MBNet.

- Se o cliente estiver numa loja virtual de um comerciante **aderente**, visualiza o nome do estabelecimento virtual, o montante e o código de moeda da operação, devendo de seguida confirmar o pagamento carregando na tecla OK. No final da operação obtem uma resposta positiva de pagamento efectuado com sucesso.

- Se o cliente estiver numa loja virtual de um comerciante **não aderente**, deve em primeiro lugar indicar o montante que pretende para o cartão temporário, obtendo como resposta positiva o respectivo número, a data de expiração e o CVV2/CVC2, para indicar no *site* do comerciante.

O *pop up* MBNet, a Identificação e o Código Secreto MBNet são sempre comunicados entre o computador do cliente e o sistema central da SIBS recorrendo a cifras com base num algoritmo de segurança.

O cliente pode errar o seu Código Secreto MBNet, no máximo, três vezes consecutivas, a partir da qual deve efectuar um *reset* desse Código Secreto. Pode fazer esse *reset* através da operação "2ª via de Talão MBNet" no serviço MBNet do Caixa Automático Multibanco ou solicitando directamente ao Emissor.

Este procedimento pode ser executado no máximo nove vezes. A partir deste número, a sua Identificação MBNet fica inibida de utilização, tendo (se assim o pretender) de efectuar uma nova adesão para poder continuar a utilizar o serviço.

Matriz de utilização do Serviço

	Comerciante	
	Aderente ao MBNet	Não Aderente ao MBNet
Cliente	Efectuado num TPA Virtual com Id. MBNet + Código Secreto	Efectuado com Cartão Temporário, atribuído a uma Id. MBNet + Código Secreto

D.1.4.1 DESCRIÇÃO DAS OPERAÇÕES EM COMERCIANTES ADERENTES

D.1.4.1.1 PEDIDO DE AUTENTICAÇÃO MBNet

Ocorre quando um cliente pretende efectuar um pagamento na Internet. É sempre efectuado directamente pelo cliente no *pop up* MBNet.
Só pode ser efectuado por um cliente que já tenha aderido ao serviço MBNet, caso contrário é recusado.

Os dados do cliente (Identificação e Código Secreto MBNet) são comunicados do computador do cliente até ao sistema central sempre codificados.
O pedido de autenticação MBNet tem a validade de **1 hora**, durante a qual deve chegar um pedido de autorização, caso não ocorra, o pedido de autenticação é apagado do sistema.
Está sempre associado a um TPA virtual que tem um acordo de representação para aceitação da operação de autorização.

Exemplo de um pedido de autenticação MBNet:

1. É solicitado ao cliente (ver **figura 5**):
   - a Identificação MBNet
   - o Código Secreto MBNet

2. Os dados introduzidos pelo cliente (Identificação MBNet e Código Secreto) são validados, assim como a situação que lhe está associada.

    - Se os dados do cliente são aceites:
      O servidor aplicacional valida a existência dos dados do comerciante (TPA) aderente;
    - Se os dados do cliente são recusados:
      O servidor aplicacional recusa a autenticação, apresentando o motivo ao cliente.

3. Se os dados do cliente foram aceites, o sistema valida a existência e situação do TPA virtual.

    - Se o TPA está válido, o sistema apresenta no ecrã do computador do cliente, os seguintes dados da operação: nome do estabelecimento virtual, referência e montante;
    - Se o TPA não está válido, o sistema apresenta uma mensagem de recusa, indicando o motivo ao cliente.

4. Se os dados do TPA foram aceites, o sistema valida o montante máximo indicado pelo cliente para a utilização da sua Identificação MBNet face ao valor da autorização.

    - Se a operação foi aceite:
      O sistema responde com uma mensagem de aceitação, atribuindo uma referência única à operação que não é visível para o cliente;
    - Se a operação foi recusada:
      O sistema responde com uma mensagem de erro, apresentando o motivo ao cliente.

D.1.4.1.2 AUTORIZAÇÃO MBNet

A autorização MBNet é processada após um correspondente pedido de autenticação MBNet aceite. Apresenta sempre o mesmo valor que o pedido de autenticação, caso contrário é recusada.

Valida o montante máximo posicionado pelo cliente para a sua Identificação MBNet face ao valor da autorização e actualiza o montante que o cliente ainda pode usar no dia.

O sistema de pagamentos atribui uma chave única à Autorização MBNet.

Para o Emissor, gera um cativo na conta do cliente. Este cativo tem por objectivo garantir a não repudiação da operação por parte do cliente, quando ocorrer a operação de compra após autorização.

Esta serve para uma única compra, que pode ter um valor igual ou inferior ao da autorização original. Se tiver um valor inferior, o sistema desencadeia automaticamente uma operação de cancelamento da autorização pelo total e permite que o comerciante efectue uma nova autorização pelo remanescente.

A autorização deixa de ser válida quando:

- A data da operação de autorização mais 30 dias de calendário, for superior à data corrente;
- Ocorrer uma operação de compra após autorização;
- Ocorrer uma operação de cancelamento de autorização.

D.1.4.1.3 CANCELAMENTO DE AUTORIZAÇÃO MBNet

O cancelamento só é possível após um correspondente pedido de autorização aceite. Se a autorização ainda não tiver nenhuma operação de compra, o valor do cancelamento deve ser igual ao da correspondente autorização, caso contrário, é o valor remanescente.

D.1.4.1.4 COMPRA APÓS AUTORIZAÇÃO MBNet

Um pedido de compra após autorização pode ser efectuado após um correspondente pedido de autorização aceite e não cancelado. O valor de uma compra após autorização pode ser igual ou inferior ao da correspondente autorização.

D.1.4.1.5 DEVOLUÇÃO DE COMPRA APÓS AUTORIZAÇÃO

Um pedido de devolução de compra pode ser efectuado após um correspondente pedido de compra aceite. O valor da devolução pode ser igual ou inferior ao da correspondente compra após autorização.

D.1.4.2 DESCRIÇÃO DAS OPERAÇÕES EM COMERCIANTES NÃO ADERENTES

D.1.4.2.1 PEDIDO DE AUTENTICAÇÃO PARA CARTÃO TEMPORÁRIO

Este pedido ocorre quando um cliente pretende realizar um pagamento na Internet e está perante um comerciante que não é aderente ao MBNet. É sempre efectuado directamente pelo cliente no *pop up* MBNet, desde que o mesmo já tenha aderido ao serviço MBNet, caso contrário é recusado. Ver **figura 9**.

Os dados do cliente (Identificação e Código Secreto MBNet) são comunicados do computador do cliente até ao sistema central sempre codificados.

Ao BIN temporário indicado pelo Emissor do cartão real é atribuído um número de cartão temporário. Este número é único para o BIN e é gerado de forma aleatória.
A este cartão temporário é atribuída uma data de expiração inferior ou igual à data de expiração do cartão real, num máximo de 30 dias de calendário a partir da data corrente da operação, e um CVV2/CVC2 utilizando as chaves de segurança do Emissor.

D.1.4.2.2 AUTORIZAÇÃO COM CARTÃO TEMPORÁRIO

A autorização efectuada com cartão temporário é sempre processada *online* pela SIBS. Um cartão temporário tem a validade máxima de 30 dias, durante o qual deve chegar um pedido de autorização do sistema de pagamento correspondente; caso não ocorra, o cartão é apagado do sistema central.

Um cartão temporário tem um máximo de 4 utilizações, ou seja, permite-se a existência de 4 autorizações para um mesmo cartão temporário.
Um cartão temporário tem um montante máximo obrigatório definido pelo cliente no momento do pedido, que é validado contra o montante máximo indicado para a sua Identificação MBNet.

Um pedido de autorização com cartão temporário é automaticamente recusado pelo sistema se:

- Já foi ultrapassado o tempo máximo permitido para a utilização (ou seja, se já se encontra esgotado o tempo de utilização);
- Já foi utilizado o montante máximo definido pelo cliente;
- Já tem 4 utilizações aceites;
- A data de expiração não for igual à fornecida ao cliente;
- O CVV2/CVC2 não for igual ao indicado ao cliente;
- O montante for superior ao indicado pelo cliente.

Exemplo de um pedido de autenticação para Cartão Temporário:

1. É solicitado ao cliente:
   - a Identificação MBNet
   - o Código Secreto MBNet

2. Os dados introduzidos pelo cliente (Identificação MBNet e Código Secreto) são validados, assim como a situação que lhe está associada.

   - Se os dados do cliente são aceites:
     Solicita-se que o cliente introduza um montante máximo para a utilização do cartão temporário que vai ser atribuído.

     - Se o montante indicado é aceite (o sistema valida que o montante máximo indicado pelo cliente não ultrapassa o montante máximo disponível no dia para utilização no MBNet), o sistema apresenta:
       - Um número de cartão temporário
       - Uma data de expiração
       - Um CVV2/CVC2
     - Se o montante indicado não é aceite, o sistema apresenta:
       Uma mensagem de recusa, indicando o motivo ao cliente.

   - Se os dados do cliente são recusados:
     O servidor aplicacional recusa a autenticação, apresentando o motivo ao cliente.

Para as operações efectuadas em comerciantes não aderentes (cartão temporário), os códigos de operação utilizados dependem das características do Emissor.

CÓDIGOS UTILIZADOS PARA CADA UM DOS GRUPOS POSSÍVEIS

Para Emissores com processamento de mensagens *Real-Time* e do ficheiro de *Clearing* dos Sistemas de Pagamento Internacionais na SIBS.

ORIGEM	CODTRN-E (699)	TIPOTERM (003)	TIPOAUT (005)	DESCRIÇÃO	INFORMAÇÃO RECEBIDA PELO EMISSOR
SIBS - RT (msg **1161**)	012	D	35 ou 38	Autorização	Cartão real e cartão temporário
SIBS - Batch (**MDST5**)	012	D	35 ou 38	Autorização	Cartão real e cartão temporário
SIBS - RT (msg **2161**)	012	D	35 ou 38	Anulação de Autorização	Cartão real e cartão temporário
SIBS - Batch (**MDST5**)	012	D	35 ou 38	Anulação de Autorização	Cartão real e cartão temporário
SIBS - Batch (**MDST5**)	010	D	35 ou 38	Compra Após Autorização	Cartão real e cartão temporário
SIBS - Batch (**MDST5**)	0C0	D	35 ou 38	Devolução Compra Após Autorização	Cartão real e cartão temporário

Nota:
Para Emissores que não recebem o pedido de Autorização em *Real-Time* mas sim em mensagem de

Consulta de Saldos e Movimentos, onde está "(msg **1161**)" deve ler-se "(msg **1162**)".

Para Emissores com processamento de mensagens de autorização na SIBS e processamento dos ficheiros de *Clearing* dos Sistemas de Pagamento Internacionais interno.

ORIGEM	CODTRN-E (699)	TIPOTERM (003)	TIPOAUT (005)	DESCRIÇÃO	INFORMAÇÃO RECEBIDA PELO EMISSOR
SIBS - RT (msg **1161**)	012	D	35 ou 38	Autorização	Cartão real e cartão temporário
SIBS - Batch (**MDST5**)	012	D	35 ou 38	Autorização	Cartão real e cartão temporário
SIBS - RT (msg **2161**)	012	D	35 ou 38	Anulação de Autorização	Cartão real e cartão temporário
SIBS - Batch (**MDST5**)	012	D	35 ou 38	Anulação de Autorização	Cartão real e cartão temporário
Sistema de Pagamento - *clearing* (batch; ex: BASE II, ECCF)				Compra Devolução	Cartão temporário

D.1.4.3 DESCRIÇÃO DO FUNCIONAMENTO DAS OPERAÇÕES

D.1.4.3.1 UTILIZAÇÃO DO MBNet EM COMERCIANTES ADERENTES

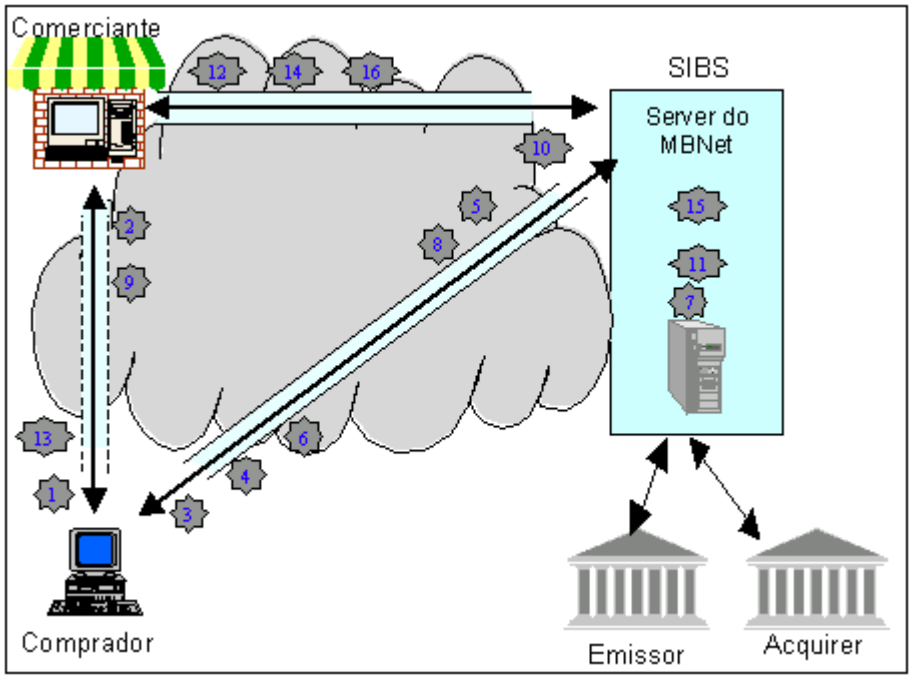


Figura 1

Legenda da figura 1:

1. O cliente estabelece uma ligação ao *site* do comerciante, onde escolhe os produtos/serviços que pretende comprar/usufruir.

2. O cliente termina as suas compras e o comerciante informa-o dos meios de pagamento que aceita, onde apresenta também o MBNet.
   Após selecção do meio de pagamento MBNet pelo cliente, a página do comerciante envia um *form* para o sistema MBNet, onde estão posicionados os seguintes parâmetros (o comerciante pode posicionar mais):

   - Número de TPA virtual
   - Referência da operação dada pelo comerciante
   - Montante da operação
   - Código de moeda do montante
   - URL do comerciante

   Com base no *form* recebido, o sistema MBNet envia os elementos da operação ao cliente (para controlo da compra) e escreve uma *cookie* no disco do PC.

3. O cliente acede ao MBNet (*pop up* de pagamento) mediante uma das seguintes opções:

   - Clicando no ícone MBNet previamente instalado no *browser* ou na barra de ferramentas (sem necessidade de sair do *site* do comerciante);
   - Escolhendo a opção MBNet, que previamente colocou no menu *Favorites* do *browser* Microsoft Internet Explorer ou no menu *Bookmark* do *browser* Netscape Navigator;
   - Digitando o endereço do *site* MBNet na barra *Address* do *browser*.

4. No *pop up* do MBNet é solicitada a introdução da Identificação e Código Secreto MBNet.

5. Após a resposta positiva do sistema, o MBNet disponibiliza ao cliente a informação sobre a operação que pretende efectuar, exibindo:

   - O nome do estabelecimento virtual
   - A referência dada pelo comerciante à operação
   - O montante e o código de moeda da operação

   Solicita-lhe ainda que confirme a operação de **Autenticação** na tecla OK.

6. Após a confirmação na tecla OK, o *browser* do cliente envia os dados para o *server* do MBNet.

7. O sistema MBNet valida a consistência dos dados e trata a operação de autenticação.

8. O sistema envia a resposta para o *browser* do cliente.

9. Ao receber uma resposta positiva, o *browser* do cliente faz automaticamente o *link* para a URL da página de confirmação da encomenda, indicada pelo comerciante.

   Desta forma, o comerciante tem conhecimento do resultado da operação de autenticação e pode apresentar ao cliente uma página do seu *site* onde lhe confirma a encomenda e apresenta outros dados, tais como a data de entrega.

10. O comerciante recebe os dados e inicia uma sessão segura com o *server* do MBNet, enviando uma mensagem de **Autorização** com os seguintes dados:

    - O número do TPA virtual
    - A referência da operação dada pelo comerciante
    - A referência MBNet da operação
    - O montante da operação
    - O código de moeda do montante
    - O certificado de comerciante

11. O *server* do MBNet recebe os dados e processa-os, tendo em conta a operação de autenticação que tem pendente.
    O sistema central valida e trata a mensagem recebida de modo semelhante a uma autorização num TPA "normal".

12. O *server* envia a mensagem de resposta (à Autorização) ao comerciante - sem os dados do cliente.

13. O comerciante dá conhecimento da resposta da operação de Autorização ao cliente.

14. Após o envio dos bens adquiridos para o cliente, o comerciante envia a mensagem de **compra após autorização** para o *server* do MBNet, repetindo-se os passos 11 a 13 na perspectiva da operação de compra após autorização.

15. O sistema MBNet recebe e trata a operação de compra após autorização, tendo em conta a operação original de autorização.

16. Por fim, o sistema responde o resultado da operação de compra ao comerciante.

D.1.4.3.2 UTILIZAÇÃO DO MBNet EM COMERCIANTES NÃO ADERENTES

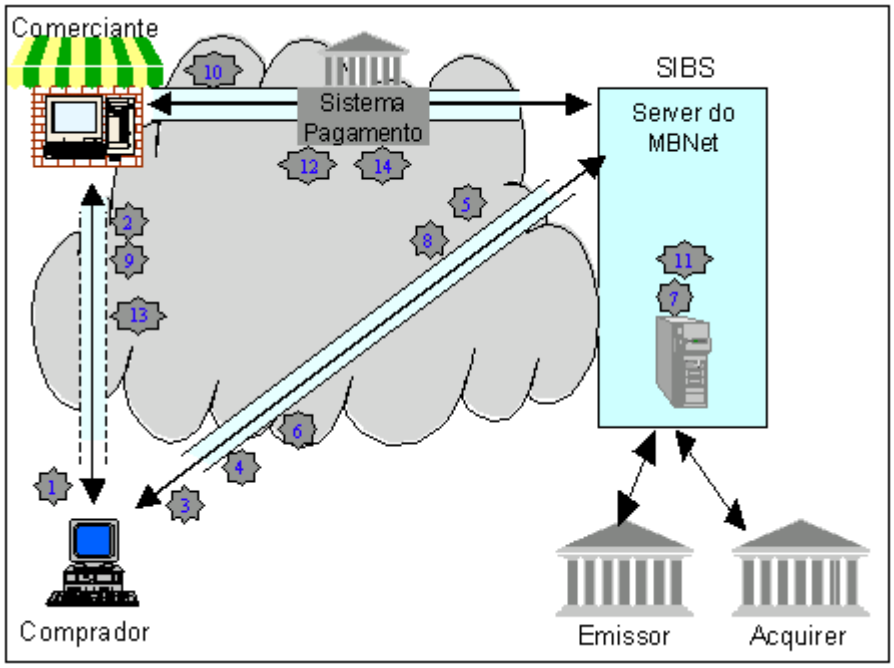


Figura 2

Legenda da figura 2:

1. O cliente estabelece uma ligação ao *site* do comerciante, onde escolhe os produtos/serviços que pretende comprar/ usufruir.

2. O cliente termina as suas compras e o comerciante informa-o dos meios de pagamento que aceita, devendo aquele escolher a opção de pagamento com cartão de crédito da marca do seu.

3. O cliente acede ao MBNet (*pop up* de pagamento) mediante uma das seguintes opções:

   - Clicando no ícone MBNet previamente instalado no *browser* ou na barra de ferramentas (sem necessidade de sair do *site* do comerciante);
   - Escolhendo a opção MBNet, que previamente colocou no menu *Favorites* do *browser* Microsoft Internet Explorer ou no menu *Bookmark* do *browser* Netscape Navigator;
   - Digitando o endereço do *site* MBNet na barra *Address* do *browser*.

4. No *pop up* do MBNet, é solicitada a introdução da Identificação e Código Secreto MBNet.

5. Após a resposta positiva do sistema, o MBNet solicita ao cliente a introdução do Limite de Utilização - para aquele pagamento - em euros.
   O cliente introduz o limite solicitado e confirma com a tecla OK.

6. Após a confirmação na tecla OK, o browser do cliente envia os dados para o *server* do MBNet.

7. O sistema MBNet valida a consistência dos dados e, caso a operação seja aceite, atribui um cartão temporário.

8. O sistema envia a resposta positiva para o *browser* do cliente, mostrando no *pop up*:

   - Um número de cartão temporário
   - Uma data de expiração do cartão temporário
   - Um CVV2 / CVC2

9. O cliente, tendo por base os dados recebidos no *pop up* MBNet, introduz no *site* do comerciante o número de cartão temporário, a respectiva data de expiração e o CVV2/CVC2 (nem todas as lojas virtuais solicitam a indicação do CVV2/CVC2).

10. O comerciante recebe os dados e envia uma mensagem de pedido de autorização, através do seu *Acquirer*, para o Sistema de Pagamento Internacional (Visa/MasterCard/AMEX) que por sua vez envia a mensagem de autorização para a SIBS com os seguintes dados:

    - Número de cartão temporário
    - Data de expiração do cartão
    - CVV2 / CVC2 (se indicado pelo cliente)
    - Montante da operação
    - Código de moeda do montante da operação

11. A SIBS recebe o pedido de autorização, valida que é um cartão temporário válido que atribuiu a um determinado cartão real e processa o pedido de autorização.

12. A SIBS envia a resposta ao pedido de autorização para o sistema de pagamento, que por sua vez a encaminha para o comerciante.

13. O comerciante dá conhecimento da resposta da operação de Autorização ao Cliente.

14. Após o envio dos bens adquiridos para o cliente, o comerciante envia a operação de compra após autorização para o *Acquirer*, sendo esta encaminhada pelo Sistema de Pagamento Internacional através do ficheiro de *Clearing* (ex: BASE II, EECF) para a entidade indicada pelo Emissor àquele sistema.

EXEMPLO DA UTILIZAÇÃO DO SERVIÇO NUM COMERCIANTE ADERENTE:

O cliente define o seu cesto de compras no *site* do comerciante e confirma a encomenda, seleccionado de seguida o MBNet como forma de pagamento.

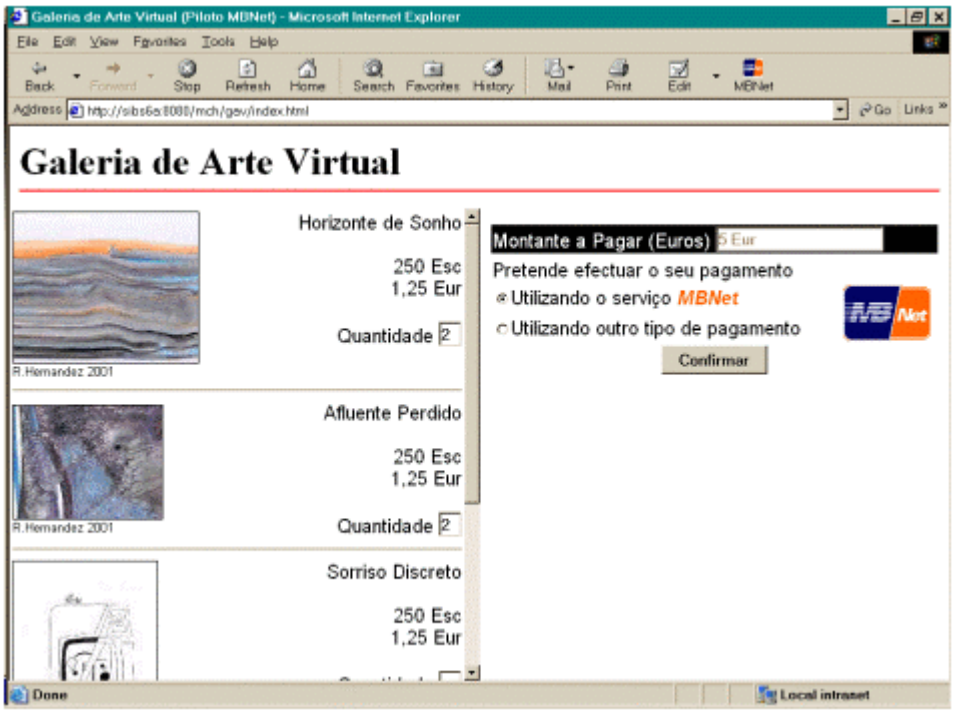


Figura 3

Para efectuar o pagamento da encomenda, basta ao cliente fazer um clique no ícone MBNet previamente instalado no *browser* ou na barra de ferramentas (sem necessidade de sair do *site* do comerciante - em alternativa pode sempre aceder ao *site* MBNet e seleccionar o botão "GO").

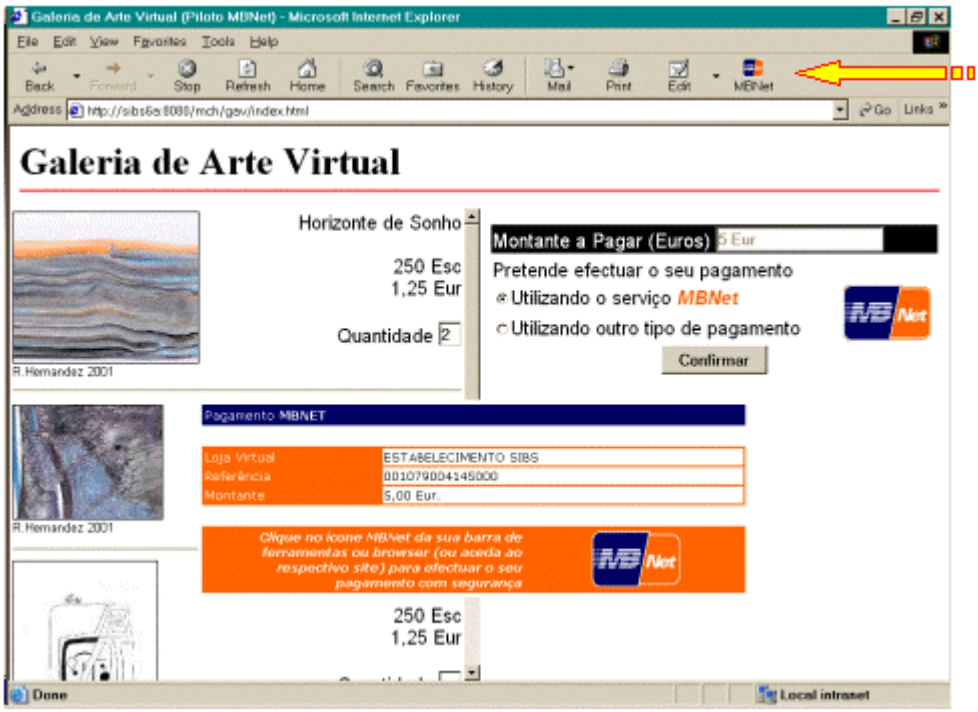


Figura 4

Ao fazer um clique no ícone MBNet, abre-se uma pequena janela - *pop up* - onde se pode dar seguimento ao processo de pagamento.

O cliente solicita a autenticação no sistema, através da sua Identificação e Código Secreto MBNet.

Após a introdução dos dados, confirma na tecla OK.

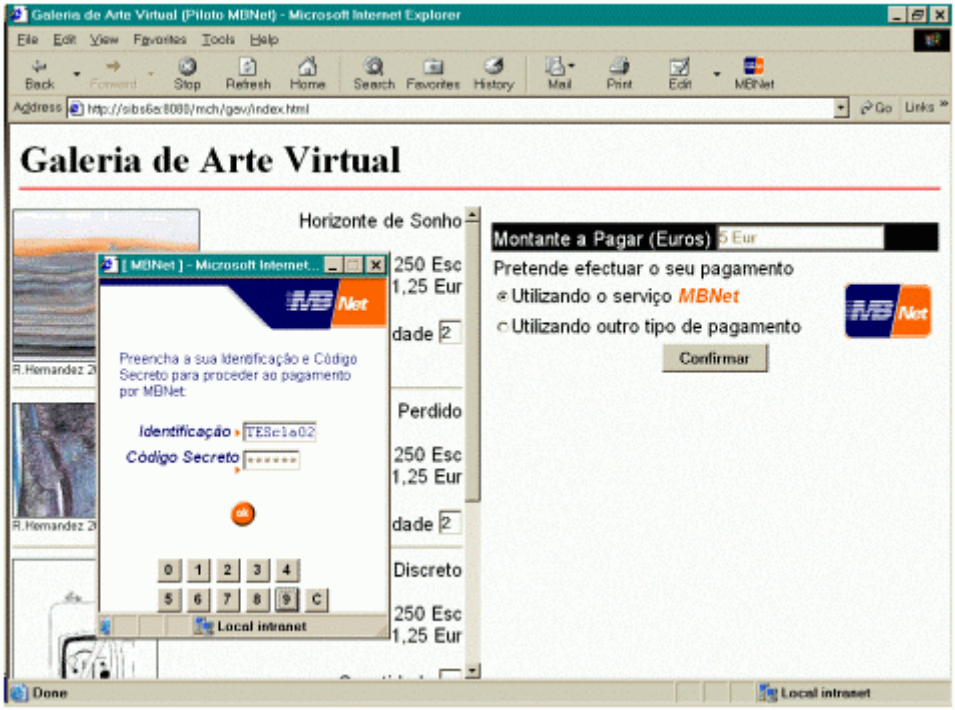


Figura 5

Como resposta positiva do sistema, o cliente visualiza no *pop up* a identificação da loja virtual, a referência da operação dada pelo comerciante, o montante e o código de moeda da operação.

Caso os dados apresentados estejam correctos, o cliente deve confirmar através da tecla OK.

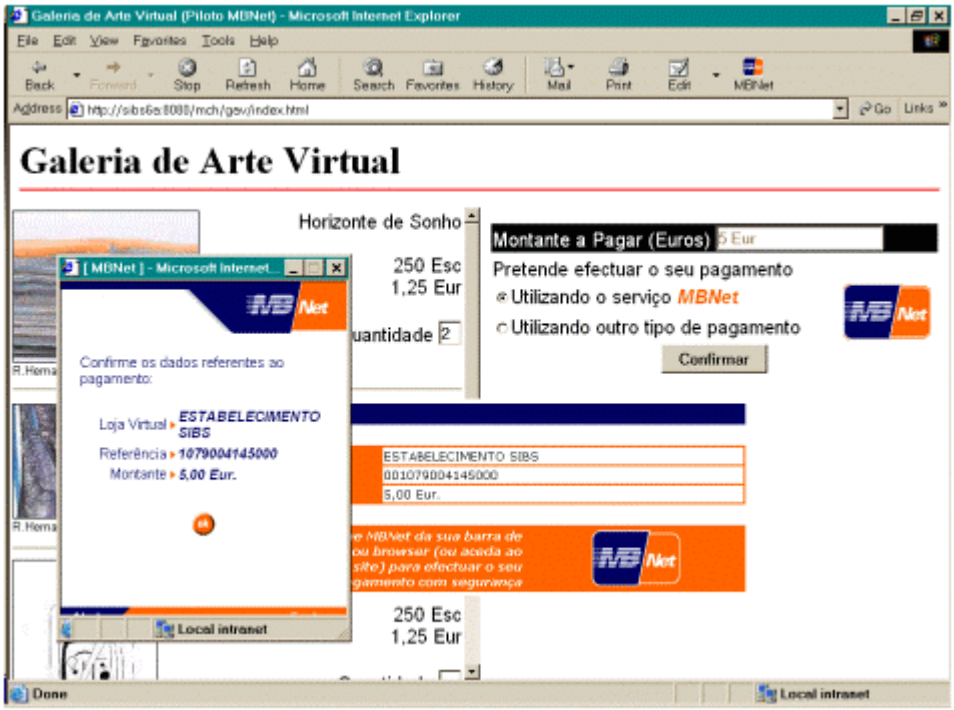


Figura 6

Após o OK, o cliente visualiza um *pop up* de confirmação dos dados e retorna ao *site* do comerciante.

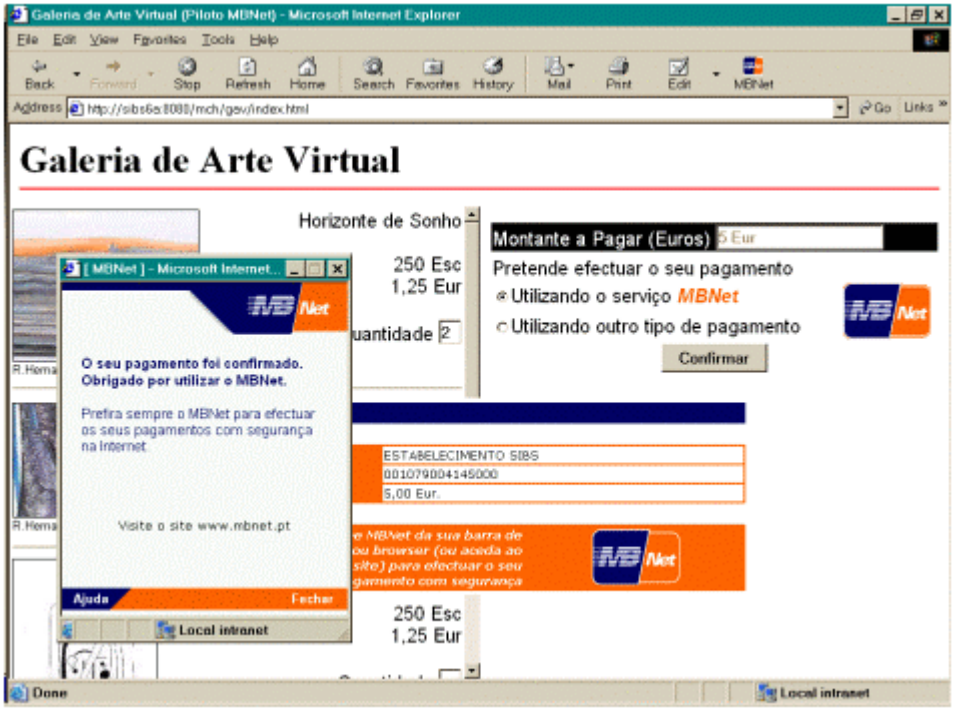


Figura 7

EXEMPLO DA UTILIZAÇÃO DO SERVIÇO NUM COMERCIANTE NÃO ADERENTE:

Num comerciante não aderente ao serviço MBNet, este apresenta ao cliente os meios de pagamento aceites e solicita a introdução dos dados do cartão.

Para efectuar o pagamento da encomenda, basta ao cliente fazer um clique no ícone MBNet previamente instalado no *browser* ou na barra de ferramentas (sem necessidade de sair do *site* do comerciante - em alternativa pode sempre aceder ao *site* MBNet e seleccionar o botão "GO").

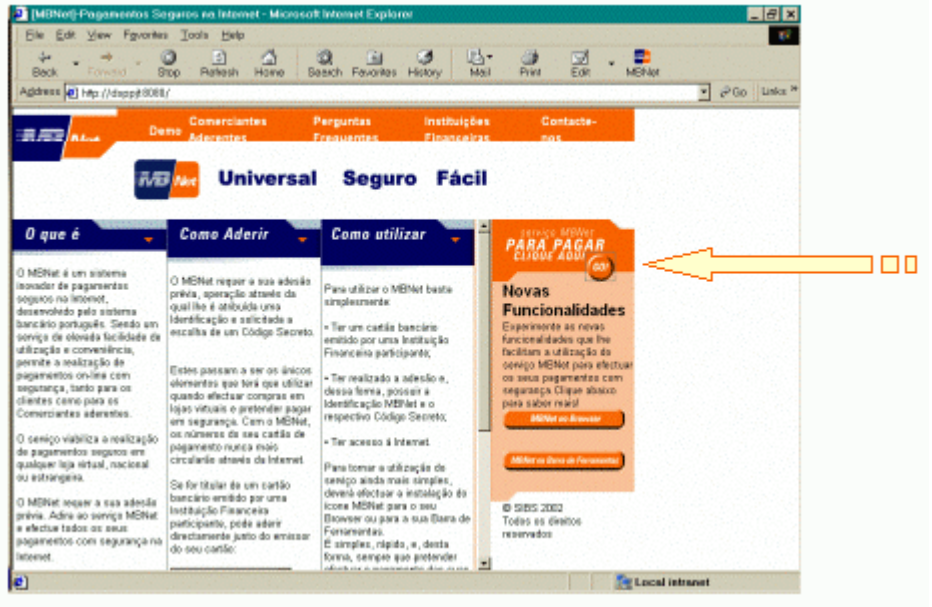


Figura 8

Ao fazer um clique no ícone MBNet, abre-se uma pequena janela - *pop up* - onde se pode dar seguimento ao processo de pagamento.

O cliente solicita a autenticação no sistema, através da sua Identificação e Código Secreto MBNet.

Após a introdução dos dados, confirma na tecla OK.

Figura 9

O sistema MBNet identifica que a operação vai ser efectuada num comerciante não aderente e solicita ao cliente a introdução do montante máximo para o cartão temporário a ser gerado (em euros). Este montante é o limite máximo de pagamento que pode ser utilizado pelo comerciante onde o cliente pretende efectuar a operação.

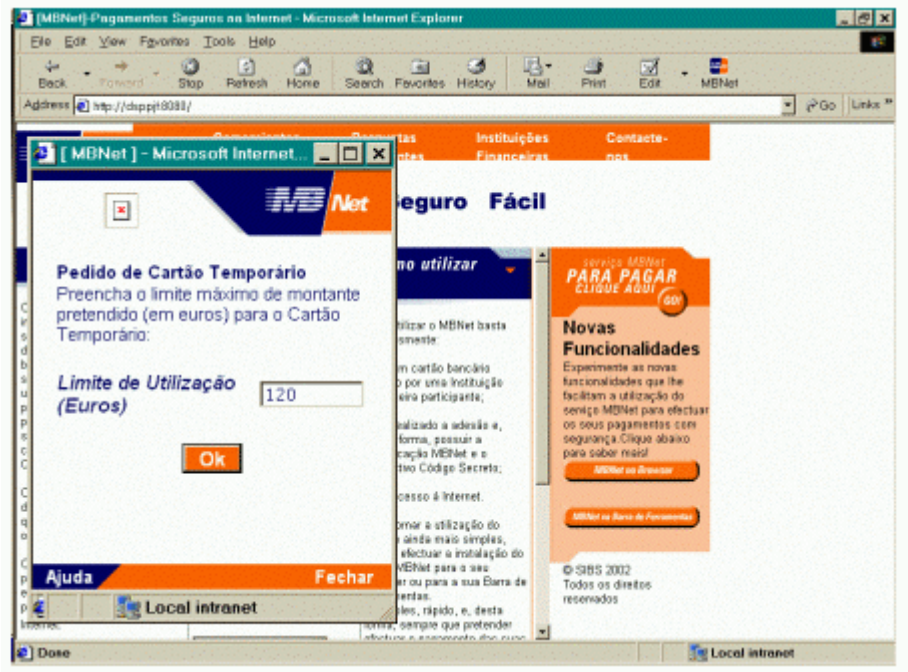


Figura 10

O cliente recebe como resposta do MBNet um número de cartão temporário, uma data de expiração e um CVV2.

Figura 11

Ao cliente basta introduzir os dados obtidos (do *pop up* MBNet) no *site* do comerciante para que este efectue a operação de autorização.

O comerciante efectua o pedido de autorização, através do seu *Acquirer*. Após obter a resposta do sistema, apresenta o resultado ao cliente.

D.1.5 SINOPSE DAS CONDIÇÕES DE PARTICIPAÇÃO NO SERVIÇO

D.1.5.1 REGISTO DE CLIENTES NO MBNet

<table>
<tr><th colspan="3"></th><th>O que o Emissor tem que fazer</th></tr>
<tr><td colspan="2" rowspan="3">No Caixa Automático Multibanco</td><td>Disponibilização do serviço</td><td>Autorizar o Serviço Especial MBNet para os seus BINs</td></tr>
<tr><td>Mensagens real-time com a SIBS</td><td>Opcional

Implementação da Mensagem Real-Time</td></tr>
<tr><td>Ficheiro Destinos (MDST5)</td><td>Tratamento do registo no ficheiro Destinos

O registo é idêntico ao enviado para outros serviços especiais, pelo que, se o Emissor não tiver um tratamento diferenciado para estas operações, não é necessário efectuar desenvolvimento informático.</td></tr>
<tr><td rowspan="2">No Emissor

Opcional</td><td>Utilização do Terminal de Serviços SIBS</td><td>Ficheiro Destinos (MDST5)</td><td>Tratamento do registo no ficheiro Destinos

O registo é idêntico ao enviado para outros serviços especiais, pelo que, se o Emissor não tiver um tratamento diferenciado para estas operações, não é necessário efectuar desenvolvimento informático.</td></tr>
<tr><td>Canal próprio do Banco</td><td>Mensagens Host-to-Host</td><td>Implementação das mensagens Host-to-Host</td></tr>
</table>

D.1.5.2 OPERAÇÕES NO MBNet

<table>
<tr><th rowspan="2"></th><th colspan="2">O que o Emissor tem que fazer</th></tr>
<tr><td colspan="2">Gestão de Cativos nas contas D.O.

Caso não tenha já implementado essa funcionalidade.</td></tr>
<tr><td rowspan="4">Mensagens real-time com a SIBS</td><td colspan="2">Mensagens 1161, 2161 e 3161</td></tr>
<tr><td rowspan="3">Códigos de transacção nas mensagens</td><td>Autorização Net - 094</td></tr>
<tr><td>Cancelamento autorização Net - 095</td></tr>
<tr><td>Compra após autorização - 027</td></tr>
<tr><td rowspan="3">Ficheiro Destinos (MDST5)</td><td rowspan="3">Códigos de transacção nos ficheiros</td><td>Autorização Net - 094</td></tr>
<tr><td>Cancelamento autorização Net - 095</td></tr>
<tr><td>Compra após autorização - 027</td></tr>
</table>

D.1.5.3 OPERAÇÕES COM CARTÃO TEMPORÁRIO - PROCESSAMENTO NA SIBS

Para Emissores com processamento de ficheiros de *Clearing* na SIBS, S.A..

	O que o Emissor tem que fazer
	Solicitar um novo BIN para cartões temporários aos Sistemas de Pagamento Internacionais.
Mensagens *real-time* com a SIBS	Nada
Ficheiro Destinos (MDST5)	Nada

D.1.5.4 OPERAÇÕES COM CARTÃO TEMPORÁRIO - PROCESSAMENTO INTERNO

Para Emissores com processamento de ficheiros de *Clearing* interno.

	O que o Emissor tem que fazer
	Solicitar um novo BIN para cartões temporários aos Sistemas de Pagamento Internacionais.
	Gestão de Cativos nas contas D.O. Caso não tenha já implementado essa funcionalidade.
Mensagens *real-time* com a SIBS	Nada
Ficheiro Destinos (MDST5)	Implementar tratamento da informação sobre cartão temporário recebida no registo da autorização, para posterior utilização no processamento do ficheiro de *Clearing* e nos posteriores casos de disputas (*chargebacks*).

D.1.5.5 REQUISITOS PARA O *POP UP* E ÍCONE MBNet

O logotipo de cada Emissor a constar do *pop up*, deve ser personalizado por Emissor e por BIN (e extensão) do Emissor, ter as dimensões 108x40 *pixels* e ser em formato JPEG. A gestão/actualização dos JPEGs é sempre da responsabilidade do Emissor.

Figura 12

D.1.5.5.1 REQUISITOS PARA A INSTALAÇÃO, OU REMOÇÃO, DO ÍCONE MBNet A PARTIR DOS EMISSORES

Para as opções de instalação ou remoção do ícone MBNet, o Emissor deve incluir o seguinte *link* nas páginas de *download*:

https://www.mbnet.pt/cc/pop_install.html
(aconselha-se a ser aberto numa janela/área de 370 por 350 *pixels*)

D.1.5.5.2 REQUISITOS PARA A CONSULTA DE OPERAÇÕES MBNet A PARTIR DOS EMISSORES

Os *links* que possibilitam a consulta de operações MBNet a partir dos *sites* dos Emissores são:

- Certificação
  https://cer.pnet.multibanco.pt/cns/index.html

- Produção
  https://www.mbnet.pt/cns/index.html

Os Emissores podem optar por uma das duas formas de apresentação destas consultas.

- **Opção 1 - Abrir um *pop up* com as seguintes características:**

  - toolbar=no
  - location=no
  - status=yes
  - menubar=no
  - scrollbars=no
  - resizable=no
  - width=780
  - height=520

  Exemplo em 'JavaScript'

```
window.open('https://www.mbnet.pt/cns/index.html','cnsmbnet','toolbar=no,location=no,
status=yes,menubar=no,scrollbars=no, resizable=no,width=780,height=520')
```

- **Opção 2 - Abrir uma *frame* do *site* com as seguintes características:**

  - width=780
  - height=520

Seguinte

D.2 SERVIÇOS DE ACESSO AO MULTIBANCO

O serviço de Acesso Multibanco (AMB), lançado em 1992, teve como objectivo permitir que os clientes possuidores de cartões Multibanco pudessem utilizar o seu cartão para pagar bens ou serviços, consultar a sua conta, consultar os movimentos efectuados com o seu cartão ou outras funções disponibilizadas por cada Emissor.

Estes serviços eram acedidos através de terminais não directamente relacionados com nenhuma instituição bancária e certificados pela SIBS. O aparecimento e alargamento dos serviços de *homebanking*, generalizou o acesso aos clientes bancários do mesmo tipo de serviços, pelo que o AMB é descontinuado em Abril de 2005.

Anterior/Seguinte

D.3 AUTENTICAÇÃO FORTE

O Sistema de Autenticação Forte é um serviço, disponibilizado pela SIBS a entidades bancárias e não bancárias, que possibilita a autenticação segura de um cliente em canais como a Internet.

A Autenticação Forte baseia-se na infra-estrutura de segurança descrita na especificação CAP (*), que por sua vez se baseia na segurança existente na norma EMV para cartões bancários. Desta forma, no âmbito da Autenticação Forte, é possível utilizar cartões bancários EMV para realizar operações de autenticação.

(*) CAP = *Chip Authentication Program* (norma definida pela MasterCard e adoptada pela VISA para autenticação forte *online*, baseada na utilização de cartões com *chip* EMV).

D.3.1 ENQUADRAMENTO

Nas operações em que existe um processo de autenticação de um cliente por canais como a Internet (exemplo: acesso a *Home Banking*), as *passwords* dos clientes podem ser comprometidas através de:

- engenharia social;
- *phishing*;
- *keyloggers* (e outros *loggers*);
- cavalos de Tróia (*trojans*).

Considerando em particular o impacto relativo a operações em *Home Banking*, estes ataques podem comprometer:

- a confidencialidade da informação;
- a integridade das transacções financeiras;
- o património dos clientes e do banco;
- a confiança dos clientes e a imagem dos bancos.

Num contexto em que é visível uma tendência de crescimento da frequência e sofisticação dos ataques, é cada vez mais necessário considerar mecanismos de assinatura das transacções ou de confirmação das transacções que (a) funcionem fora do contexto de segurança do cliente ou (b) por canais alternativos.

Para dar resposta às necessidades crescentes de definição de mecanismos de assinatura de transacções, e após análise das diversas alternativas disponíveis, a opção de implementação de um novo sistema recaiu na utilização do padrão EMV-CAP.

A opção pela utilização do padrão EMV-CAP resulta das vantagens que podem ser obtidas pela rentabilização dos seguintes factores:

- capitalização do projecto EMV;
- possibilidade de conjugar a segurança do *eBanking* e do comércio electrónico;
- potencial atractividade para outras entidades, em particular na área do *eGovernance*;
- capacidade de personalização do cartão e de partilha do leitor do cartão;
- alinhamento com tendências de mercado;
- utilização de um padrão de mercado (EMV-CAP), que permite independência de fornecedores.

Enquanto padrão aceite pelo mercado, a utilização da solução EMV-CAP como base de implementação de um Sistema de Autenticação Forte tem inerente várias vantagens:

- Capitaliza as características específicas do EMV. O CAP reutiliza estruturas de dados das aplicações de pagamentos, introduzindo novos elementos.

- Garante a interoperabilidade entre leitores e cartões, através das padrões EMV *Level* 1 (requisitos de *hardware*) e EMV *Level* 2 (requisitos de *software*).

- Permite obter evidência da:

  a. presença do cliente (*cardholder*), através da introdução de um PIN (mandatório);
  b. presença do cartão de pagamento no ponto de interacção, através da geração de um criptograma;
  c. aprovação dos detalhes da transacção, através da assinatura de campos (opcional).

- O EMV-CAP prevê diversos modos de funcionamento (incluindo *Mode 2* e o *Mode 2* com TDS, respectivamente para autenticação forte no *login* e para assinatura de transacções).

D.3.2 GLOSSÁRIO

AC	*Application Cryptogram*
AF	Autenticação Forte
BIN	*Bank Identification Number*
CAP	*Chip Authentication Program*
EMV	Europay MasterCard Visa
HSM	*Hardware Security Module*
PAN	*Primary Account Number*
PCR	*Personal Card Reader*
PIN	*Personal Identification Number*
SAF	Sistema de Autenticação Forte

D.3.3 ENTIDADES ENVOLVIDAS NA AUTENTICAÇÃO

Identificam-se de seguida as entidades envolvidas no processo de Autenticação Forte e nos processos de gestão de informação associados.

Emissor

O Emissor do cartão é responsável por desencadear o pedido de emissão de um cartão definindo a existência ou não da aplicação CAP no mesmo. Ao definir a existência da aplicação CAP no cartão, esta informação dá origem à criação no *Host* da SIBS dos elementos de informação necessários para envio ao SAF (Sistema de Autenticação Forte).
O Emissor é também responsável por solicitar a alteração de estado do cartão.

Host SIBS

O *Host* SIBS é responsável por processar os pedidos realizados pelos Emissores e produzir em conformidade os dados necessários para a personalização do cartão, gerar e comunicar a informação necessária ao SAF para responder aos pedidos de autenticação.
São também processados e comunicados por esta entidade ao SAF os pedidos de alteração de estado do cartão (aplicação CAP).

SIBS Cartões

No cenário de produção do cartão por parte da SIBS Cartões, é a entidade responsável pela produção e personalização do cartão com os elementos necessários ao processo de autenticação CAP.

WEB do Emissor

Esta entidade recebe internamente os dados relativos a um cartão, nomeadamente o PAN, e associa-os a um utilizador do seu sistema. Estes dados são enviados ao SAF na mensagem de autenticação.

Entidades Externas

Qualquer entidade fora do sistema bancário que queira utilizar o sistema AF para realizar autenticação dos seus utilizadores.
Estas entidades participam no sistema através de um Emissor ou directamente (cenário *E-Government*). Recebem por parte do Utilizador dados que o identificam no seu sistema e um *token* CAP que o autentica.
As mensagens de autenticação enviadas por estas entidades não possuem o PAN completo (apenas os últimos 4 dígitos). Adicionalmente é enviado o NIF do utilizador (previamente registado no sistema) e o NIF da entidade que indica a proveniência da mensagem de autenticação.

SAF

Este sistema tem a responsabilidade de manter a estrutura de dados necessária para a resposta a pedidos de validação de *tokens* CAP. A recepção de pedidos é feita via mensagem e realiza-se exclusivamente através de uma rede segura. A estrutura de dados é criada e gerida a partir de dados enviados por ficheiro pelo *Host* SIBS.
Pressupõe-se a utilização de um HSM para as operações de cifra e de validação de AC EMV. Pressupõe-se também a existência de uma chave de transporte carregada no SAF que permita a troca segura de elementos cifrados com o *Host* SIBS.

Utilizador

O utilizador é responsável por desencadear o processo de autenticação lendo o *token* CAP do PCR e fornecendo-o à entidade que lhe pediu a autenticação/assinatura. O utilizador é solicitado a introduzir o PIN no PCR durante o processo geração do *token* CAP.

D.3.4 INFORMAÇÃO RELEVANTE PARA A AUTENTICAÇÃO

Identifica-se de seguida a informação relevante para os processos de gestão e de autenticação.

Cartão com aplicação CAP

Consiste num cartão EMV que adicionalmente às aplicações de pagamento usuais inclui uma aplicação CAP para geração de criptogramas usados no processo de AF. Este cartão é emitido com PIN *Offline* de 4 dígitos, sendo este usado apenas no contexto da aplicação CAP para validação do Utilizador.

Token CAP

Consiste num código numérico de 7 dígitos (decimais) devolvido ao Utilizador pelo PCR, como resultado da transacção EMV realizada com a aplicação CAP do cartão.

Ficheiro de BINs e PANs

Ficheiro produzido pelo *Host* SIBS para envio ao SAF dos elementos necessários ao processo de autenticação.

Ficheiro EECB

Ficheiro de Emissão de cartões.
É produzido pelo Emissor de cartões e enviado à SIBS.
A emissão de cartões com aplicação CAP é suportada nas versões 03 ou superiores do ficheiro **EECB**.

Ficheiro EGCC

Ficheiro de Gestão de Cartões e Contas.
É produzido pelo Emissor de cartões e enviado à SIBS para alterar elementos associados ao cartão. Permite também realizar a associação entre NIF e PAN do cartão.

Ficheiro de Personalização de Cartões

Ficheiro **PEMV** - Ficheiro de Emissão de cartões para entidades de produção de cartões (que não a SIBS Cartões).
É produzido pelo *Host* SIBS e devolvido ao Emissor na sequência do processamento de um ficheiro **EECB**.
A emissão de cartões com aplicação CAP é suportada pelo ficheiro **PEMV**. Adicionalmente ao ficheiro **PEMV**, é necessário que a entidade que vai personalizar o cartão considere os valores específicos a utilizar pela aplicação CAP, indicados no Livro II, capítulo A, anexo **A.AX.5**.

D.3.5 PROCESSOS ENVOLVIDOS NA AUTENTICAÇÃO

D.3.5.1 PROCEDIMENTOS PRÉVIOS À EMISSÃO

Para que um Emissor possa emitir cartões EMV com uma aplicação de autenticação são necessários dois conjuntos de acções:

- certificação do Emissor e respectivos BINs para emissão de cartões EMV com uma aplicação de um Sistema de Pagamento;
- parametrizações específicas relativas à aplicação CAP .

Mantêm-se os procedimentos já existentes na componente relativa à certificação do Emissor junto do Sistema de Pagamento, para possibilitar a emissão de cartões EMV que possuam uma aplicação de pagamento.
As acções que o Emissor necessita desenvolver para possibilitar a emissão de cartões com *chip* EMV encontram-se documentadas no Livro II, capítulo A, anexo **A.AX.4**.

O Emissor necessita ainda de desenvolver um conjunto de acções adicionais prévias a qualquer emissão de cartões EMV com uma aplicação CAP incluída no *chip*.

Nos pontos seguintes, são indicadas as acções e procedimentos que devem ser seguidos para possibilitar a emissão de cartões EMV com uma aplicação CAP.

O anexo **D.AX.1** apresenta um resumo das acções necessárias.

Caracterização de BIN

A emissão de cartões com *chip* EMV com uma aplicação CAP não tem qualquer influência sobre a estrutura das caracterizações de BIN já existentes.
O Emissor pode utilizar os BINs já parametrizados ou solicitar a parametrização de novos BINs para emissão de cartões EMV com aplicação CAP.

Caracterização de Padrão EMV

A aplicação CAP existe como aplicação independente no *chip* de cartões EMV.
A definição das aplicações EMV a colocar no *chip* tem como requisito prévio a parametrização de um Padrão EMV correspondente, que o Emissor referencia no momento da emissão do cartão e nas acções após a personalização do mesmo.
O Emissor pode solicitar a parametrização de um Padrão EMV associado a uma aplicação CAP através do Terminal de Serviços SIBS ou, na impossibilidade de utilização deste, através do anexo **I.AX.1E**, do Livro II, capítulo I.

Os elementos presentes na Caracterização do Padrão EMV: "Sufixo de AID", "*Preferred Name*" e "Segunda linguagem suportada pela aplicação" não são aplicáveis quando se indique uma aplicação CAP. Assim, os Emissores que pretendam emitir cartões com uma aplicação CAP necessitam parametrizar apenas um ou, no limite, dois Padrões EMV:

- um Padrão EMV para emissão de cartões com *chip* que utilizem uma máscara VISA;
- um Padrão EMV para emissão de cartões com *chip* que utilizem uma máscara MasterCard.

Carregamento de chaves de Emissor por BIN

A emissão de cartões EMV com aplicação CAP obriga ao carregamento prévio de chaves de Emissor. A gestão das componentes de segurança é da competência exclusiva do Emissor e/ou Entidades em quem este delegue esta gestão.

Assim, para que seja possível emitir cartões com uma aplicação CAP, o Emissor tem que indicar à SIBS quais os BINs abrangidos. Esta indicação é efectuada através do envio à SIBS, ao Departamento de Clientes e Negócios (DCN), do formulário de "Registo de BINs no Sistema de Autenticação Forte" constante no anexo **D.AX.2**.

Com a recepção deste formulário, o Departamento de Segurança e Qualidade (SIBS) efectua a geração aleatória e carregamento das chaves necessárias.
Após efectuado o carregamento das referidas chaves, o Emissor é informado pelo DCN da conclusão deste processo.

A preparação de um BIN tem como consequência a parametrização de todas as extensões que existam ou possam vir a existir para esse BIN.

Definição de contrato de produção de cartões

Para definição dos aspectos particulares dos contratos de produção de cartões a utilizar, o Emissor deve contactar a SIBS Cartões.

D.3.5.2 EMISSÃO DE CARTÃO EMV COM APLICAÇÃO CAP

A emissão de cartões com inclusão da aplicação CAP é efectuada através do ficheiro **EECB**, versão 03 ou superior.

Para incluir a aplicação CAP no cartão, o Emissor preenche uma das ocorrências do campo (**1716**) EMV-PADRAO, presente nos registos de tipo 1 do ficheiro **EECB**.

A ocorrência do campo (**1716**) EMV-PADRAO a preencher é obrigatoriamente a última da lista de ocorrências. Ou seja, a aplicação CAP é informada por uma ocorrência posterior às correspondentes a aplicações de pagamento (Visa, MasterCard, Amex ou Multibanco).

Personalização do plástico fora da SIBS (ficheiro PEMV)

A aplicação CAP constitui-se como uma aplicação EMV que coexiste no cartão com outras aplicações EMV de pagamento. A estrutura da aplicação CAP é semelhante à de uma aplicação EMV de pagamento
Na emissão de um cartão EMV com aplicação CAP é necessário considerar elementos específicos desta aplicação. Uma vez que são constantes e uma vez que o seu valor foi definido previamente, estes campos são incorporados no conjunto de elementos considerados como "Parametrizações Genéricas EMV", consultável no Livro II, capítulo A, anexo **A.AX.5**.
O cartão a usar deve garantir que com os dados de personalização enviados no **PEMV**, o valor do IAD devolvido no comando *Generate Application Cryptogram* é determinístico, e igual ao que está definido no campo (**3138**) CAP-IAD.

Informação ao Sistema de Autenticação Forte (SAF)

Os registos de emissão de cartões do ficheiro **EECB** que sejam correctamente processados, desencadeiam o envio ao SAF de informação relativa ao cartão em causa. Esta informação representa um registo do PAN de um cartão, para utilização nas operações de AF.

Assim, temos:

Informação no tipo de registo 2 do EECB	Informação no sistema SAF
(**144**) NSITCAR = 02 (Normal)	PAN activo para sistema de autenticação

Tabela 1 - Estados do Cartão no Momento da Emissão

D.3.5.3 GESTÃO DA SITUAÇÃO DO CARTÃO EMV APÓS A EMISSÃO

Informação ao Sistema de Autenticação Forte (SAF)

Ao longo da vida útil do cartão, o Emissor pode alterar a situação do cartão EMV através do ficheiro Alteração de Situação de Cartão (**EASC**) ou através do Terminal de Serviços SIBS.
Adicionalmente, existem condições nas quais a SIBS também efectua alterações à situação do cartão, automáticas ou a pedido junto dos seus serviços de atendimento (exemplo: colocação em Lista Negra).

As alterações de situação do cartão EMV têm o seguinte impacto na informação enviada ao SAF:

Alteração de situação do cartão EMV	Informação no sistema SAF
Alteração de estado de 13 (Por Activar) para 02 (Normal)	Estado de registo de PAN alterado para "activo"
Colocação de cartão em 06 (Lista Negra) ou 07 (Lista Cinzenta)	Estado de registo de PAN alterado para "inactivo"
Alteração de estado de 06 (Lista Negra) ou 07 (Lista Cinzenta) para 02 (Normal)	Estado de registo de PAN alterado para "activo"
Colocação de cartão em (09) Anulado	Estado de registo de PAN alterado para "anulado", não podendo ser retirado desse estado.

Tabela 2 - Impacto das Alterações de Situação do Cartão

D.3.5.4 GESTÃO DO ESTADO DO REGISTO DE PAN NO SAF (FICHEIRO EGCC)

Informação ao Sistema de Autenticação Forte (SAF)

A SIBS assegura a activação directa do PAN para o serviço SAF. No entanto, o Emissor pode, se o pretender, actuar directamente sobre o estado do registo de PAN existente no SAF, através do envio à SIBS do ficheiro de Gestão de Cartões e Contas (**EGCC**), com o código de gestão 19 definido para o efeito.

Através do **EGCC**, o Emissor pode desencadear as seguintes acções:

- alterar o estado do registo de PAN para "Activo", para disponibilizar o serviço de AF para um PAN;
- alterar o estado do registo de PAN para "Inactivo", para impossibilitar a utilização de um PAN no serviço de AF.

Com o processamento do ficheiro **EGCC**, o *Host* SIBS desencadeia o envio de um ficheiro de actualização dos dados existentes no SAF.

D.3.5.5 ALTERAÇÃO À ASSOCIAÇÃO DO REGISTO DE PAN A UM NIF NO SAF (FICHEIRO EGCC)

Informação ao Sistema de Autenticação Forte (SAF)

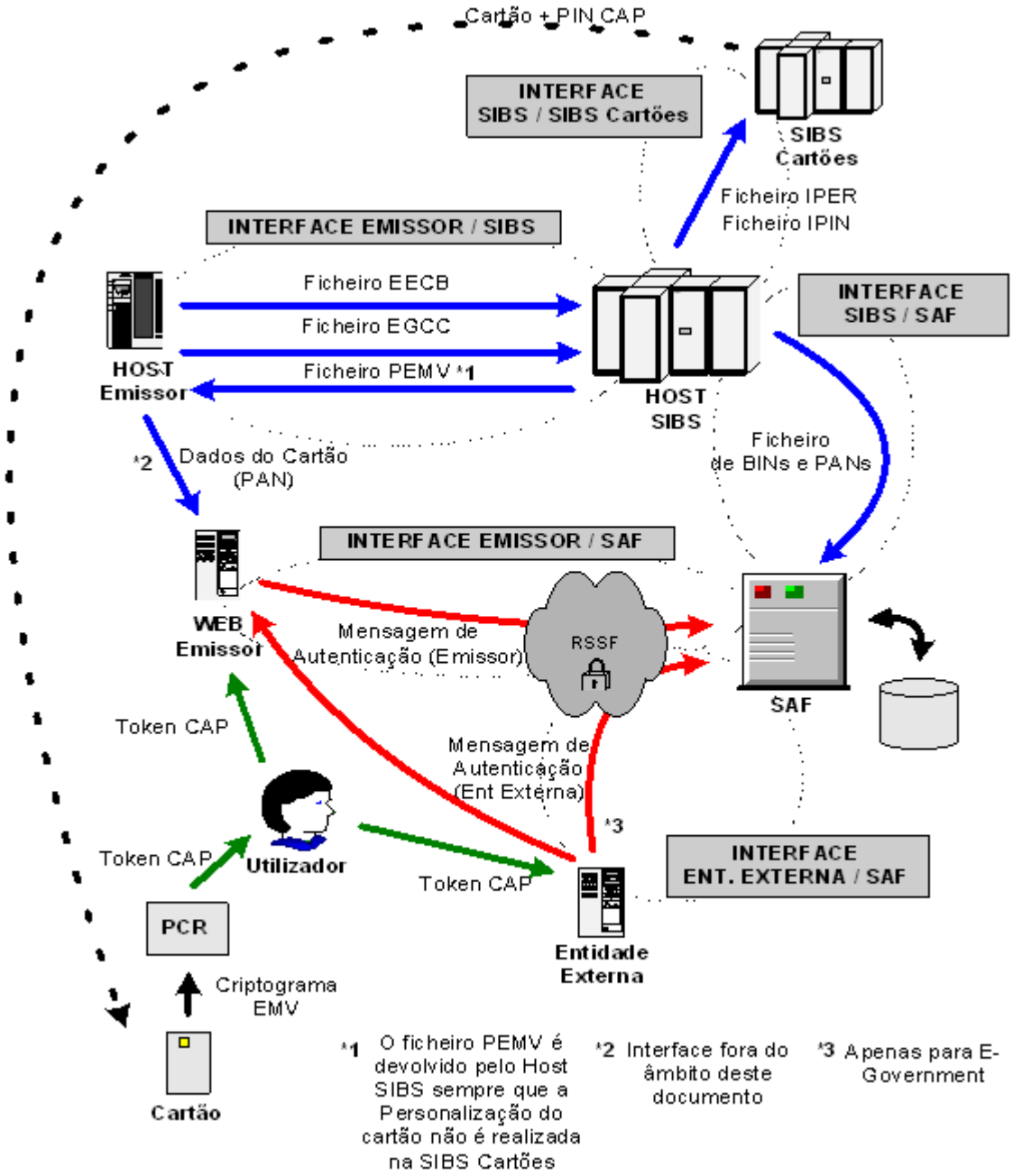
Após a emissão de um cartão EMV com aplicação CAP, o Emissor pode associar ou eliminar a associação existente entre o cartão e um Número de Identificação Fiscal.
Através desta gestão, são disponibilizadas as condições necessárias para que seja possível disponibilizar o serviço de AF a entidades não bancárias.
A gestão da associação entre os dados de um cartão e NIF é efectuada através do código de gestão 20 definido para o efeito, no ficheiro **EGCC**.

D.3.5.6 VALIDAÇÃO DO *TOKEN CAP*

Este processo é efectuado no SAF.

D.3.6 *WORKFLOW*

A figura seguinte ilustra a interacção entre os intervenientes nos processos envolvidos na Autenticação. São também evidenciados os interfaces referidos nas secções anteriores. Por questões de simplicidade é apenas apresentado um Emissor e um cartão.



D.3.7 INTERFACE EMISSOR / SIBS

Ficheiro de Emissão de Cartões (EECB)

Para a emissão de cartões EMV com aplicação CAP pode ser utilizada a versão 03 ou superior do ficheiro **EECB**.

Ficheiro de Personalização de Cartões EMV (PEMV)

A aplicação CAP obedece à estrutura das aplicações EMV de pagamento, pelo que os dados para personalização são enviados através do ficheiro **PEMV** à semelhança das aplicações de pagamento.
Os elementos específicos da aplicação CAP têm um valor pré-determinado. São por isso englobados no conjunto de elementos considerados como "Parametrizações Genéricas EMV", apresentadas no Livro II, capítulo A, anexo **A.AX.5**.

Ficheiro de Gestão de Cartões e Contas (EGCC)

Para possibilitar a gestão da informação que vai residir no SAF, são utilizados dois códigos de gestão específicos:

- CODGEST=19 - Sistema de Autenticação Forte - activa/inactiva serviço de autenticação;
- CODGEST=20 - Sistema de Autenticação Forte - alteração de associação de cartão a NIF.

D.3.8 INTERFACE EMISSOR / SAF

A forma de interacção entre o Emissor e o SAF baseia-se na troca de mensagens real-time, utilizando protocolo HTTPS - método POST.

Informação detalhada relativa a estas mensagens pode ser consultada no capítulo **D.5** do Livro III.

D.3.9 INTERFACE ENTIDADE EXTERNA / SAF

A forma de interacção entre o Emissor e o SAF baseia-se na troca de mensagens real-time, utilizando protocolo HTTPS - método POST.

Informação detalhada relativa a estas mensagens pode ser consultada no capítulo **D.5** do Livro III.

Anterior