SEPAmail[1] and its applications for TPPs

Document type	Contribution paper	Confidentiality	None
Subject	This document is an contribution paper on the way the SEPAmail system may answer the European Commission requirement to standardize the exchanges between Third Party Payment Service Providers (TPPs) and Account Servicing Payment Service Providers (AS-PSPs) while granting a high security level, and this especially through its RUBIS service allowing request of credit transfer initiation and its SAPPHIRE service enabling authentication functions. Disclaimer: This contribution paper is a free contribution of its authors and, as this stage, it does not necessarily reflect the position of their employer or of the shareholders of SEPAmail.eu		

Log of the document versions

Date	Version of the document	Action	Editor	Validation
25/04/2014	Release 1		Eric VERONNEAU Cyril VIGNET	

1. Executive Summary

Pending the adoption of the PSD2 and its transposition in national law, a Working Group set up by the European Commission proposed the following guiding principles (column on the left in chart below)[2].

The SEPAmail standard and its various applications, especially RUBIS and SAPPHIRE, answer (column on the right in chart below) those guiding principles while ensuring a security level compatible with the AS-PSP security level.

Guiding principles proposed by the European Commission	SEPAmail approach in order to comply with those requirements
"1. it should not impede, restrict or obstruct in any way the provision of payment initiation services by any licensed PSP"	SEPAmail already enables to perform credit transfer initiations (RUBIS application). The possibility to easily create new applications and new messages will enable to adapt both to services proposed by AS-PSPs and TPPs.

[1] SEPAmail is a messaging standard published under a Creative Commons licence, available at http://documentation.sepamail.eu

[2] Technical workshop on access to the payment accounts by third party payment service providers, 18 February 2014

"2. it should build on state-of-the-art strong customer authentication methods"	SEPAmail uses several authentication levels to authenticate both AS-PSP and TPP. SAPPHIRE application precisely enables to easily implement a strong customer authentication in different use cases. Each TPP/AS-PSP designs the way to authenticate its customer and thus remains entirely responsible of such authentication towards its customer and/or any third party All the SEPAmail authentication and security mechanisms use the state-of-the-art on the Internet: certificates X509, SSL, SMIME.
"3. it should not require any form of agreement, contractual or otherwise, between the TPP and the bank"	SEPAmail does not require any bilateral agreement between the TPP and the AS-PSP. Any user of SEPAmail (i.e. here TPP or AS-PSP) must enter a subscription contract with the SEPA mail Scheme Manager at the outset to become members of the SEPAmail Scheme. This Scheme Manager may then register these new members in a public SEPAmail directory, allowing them to work together without entering any sort of bilateral agreement. Incidentally, this SEPAmail public directory offers a good visibility to any new TPP member.
"4. the Account servicing PSP should be legally required to implement and support the solution"	Being an open standard, SEPAmail can easily be used by all AS-PSPs if required by law.
"5. it should be based on open common standards"	SEPAmail decided, from its start, to publish its standards under a Creative Commons license so that it may be used by as many entities as possible. In addition, the SEPAmail structure is mainly a combination of existing standards: • Internet standards (X509, SSL, SMIME) for the routing, confidentiality and authentication functions • ISO 20022 standards for business messages related to payments (pain.013, pain.014, pain.012, pain.009…) • ISO standards, especially those related to PDF to provide the end customer with a better user experience
"6. it should be user-friendly for payment service users (i.e. payers and merchants) and PSP"	SEPAmail conducted since 2010 several pilots that all provided good results in terms of acceptability by end users: Payment via credit transfer with validation by the customer through the home banking of its AS-PSP Payment via credit transfer with validation by the customer via a smartphone secured by SAPPHIRE Payment via credit transfer with validation by the customer on ATMs Furthermore, the possibility to transport in the same message XML-information and pdf documents allows to send to the customer all relevant information related to the transaction (i.e. copy of the invoice…) and thus to increase his

	understanding and management of the transaction

In addition, the use of this open and easily extendable standard enables any PSP to keep on proposing new and, in addition to existing applications.

The following chart shows the SEPAmail solutions available as of today to answer the basic needs of TPPs.

Services proposed by TPPs to the customer of the AS-PSP	SEPAmail applications to meet the need
Credit Transfer initiation request by a TPP to a PSP for a customer with systematic validation by the customer	RUBIS application enabling to initiate a credit transfer from a settlement request message in the ISO 20022 format (pain.013)
Credit Transfer initiation request by a TPP to a PSP on behalf of a customer, automatically validated after the beforehand enrolment of the customer	RUBIS application enabling to initiate a credit transfer from a settlement request message in ISO 20022 (pain.013) format in coordination with the SAPPHIRE application for prior authentication of the parties
Receipt of information or of account(s) statements by a TPP	Application currently being developed, based on the “camt” messages of ISO 20022

The following chart highlights the keystones of SEPAmail structure.

Scheme organisation	SEPAmail is organised around a Scheme in order simplify the contractual relationship between the members (PSP)
Public Key Infrastructure (PKI)	A PKI dedicated to the servers of members of the scheme is used to simplify and guarantee the authentication of all members. It allows members to exchange securely through the Internet.
Omni channel approach	The four corner model used by SEPAmail does not need that all corners bee on the WEB. It allows members to offer more than the web user experience to their customers
Interoperability	The multi-layers architecture of the SEPAmail standard eases the interoperability between a SEPAmail scheme and other schemes or messaging solutions. Furthermore, it allows creating more than one Scheme using SEPAmail standard.

2. Table of Contents

1. SEPAmail presentation

SEPAmail mainly includes the following concepts:

- A messaging service standards, based on the email one, but adapted to provide security, confidentiality and automation[3],
- The SEPAmail applications that already aim at providing various services meeting the needs of end users:
  - Payment via credit transfer (RUBIS)
  - Electronic direct debit orders (GEMME)
  - Payment order notification (JADE)
  - Account switching management and account data transfer (name currently being defined)
  - PDF electronic signature (JASPE)
  - Increased reliability of banking details (DIAMOND)
- An organised system (« scheme »), around a structure, SEPAmail.EU ("scheme manager") having a contract with its members (payment services providers).

The messaging service standard is released under a Creative Commons license. It is available on the website: http://documentation.sepamail.eu/wiki/Accueil.

The structuring concepts are presented in the next paragraphs.

A « 4 corners » messaging service in relation to a universal standards

The SEPAmail messaging service is a messaging service structured for « 4 corners » exchanges, which means that 2 entities exist between the sender and the recipient of the information:

- The sender messaging service interface
- The recipient messaging service interface

The SEPAmail standard defines the exchanges between the messaging service interfaces and only this. However, this standard aims at, both through its structure and its license, being also used in the relations between the interface and the sender and/or the interface and the recipient[4].

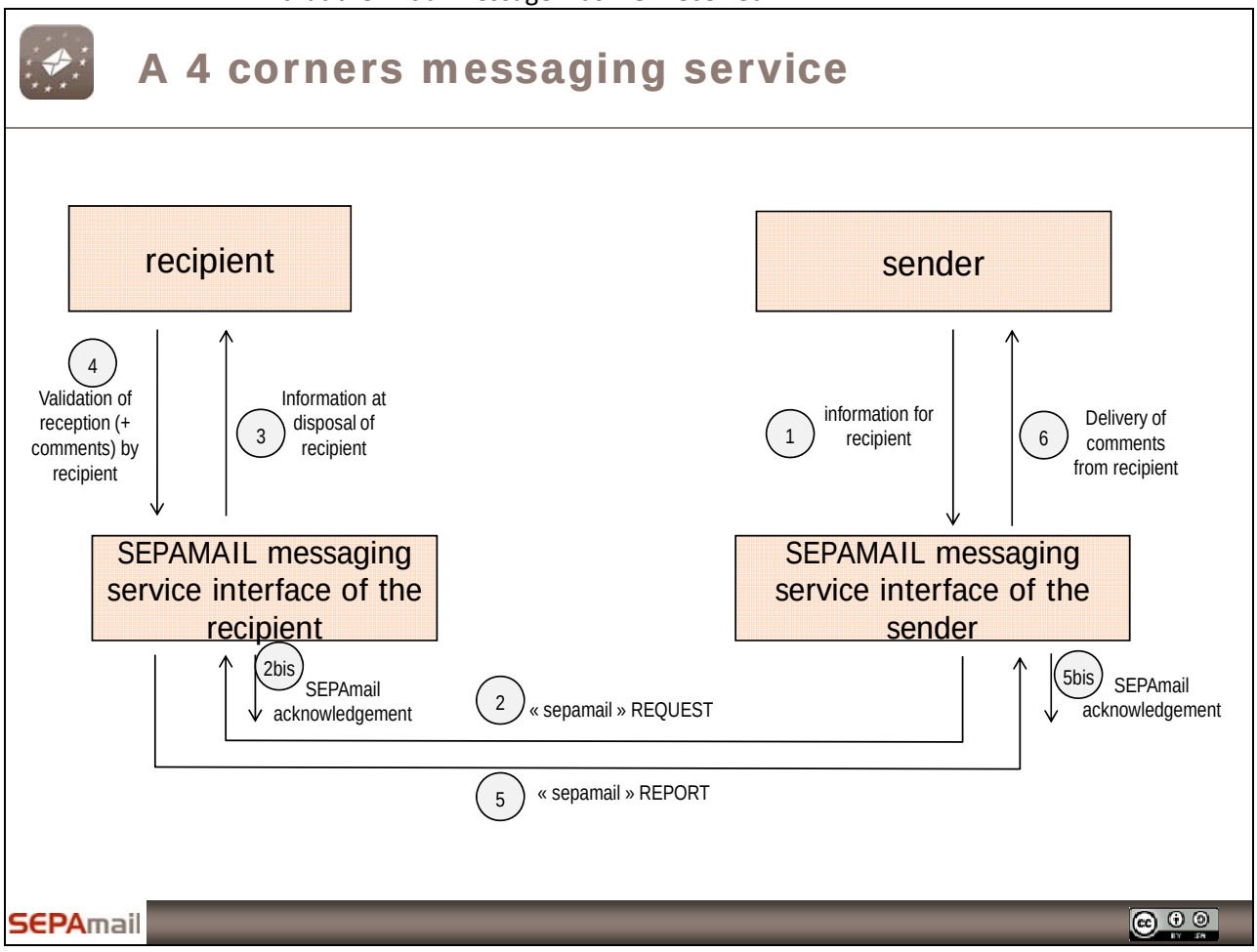
It shall be noted that the use of the standards between the interfaces is **mandatory** while the use with the senders and/or recipients is only an opportunity.

[3] Automation refers to the possibility of an automatic management by a computer, as the current email mainly targets a human user.

[4] As GOOGLE and AOL exchange emails with the « email » standards, this standards is also used for exchanges between GOOGLE and its customers. This is of course not exclusive, as if the customer uses a WEBMAIL interface, the standards used is based on the email standards.

Each « messaging service interface » is linked by a subscription contract to the Scheme Manager and undertakes, in compliance with the standards and with operational regulations, to ensure the required quality level for the messaging service:

- Available, with a 24/24-7/7 approach
- Authenticated: the recipient is authenticated, the sender is authenticated, the Members are authenticated
- Confidential: data cannot be reached by third parties other than the sender and the recipient as well as the interfaces[5]
- Traced: the trace of the message transmission is stored
- Dated: each message includes a date controlled by the « messaging service interfaces »
- Reliable: the data are not altered on the network of SEPAmail Members
- Controlled: an entity independent from interfaces, the scheme manager, controls that the messaging service is working properly
- Acknowledged: each message sent by an interface implies a message back indicating that the initial message was well received.



[5] The interfaces are anyway subject to professional secrecy

Structured exchanges between the messaging service interfaces

The previous diagram, in addition to presenting its vision of the « 4 corners » mode, shows the general structure of exchanges:

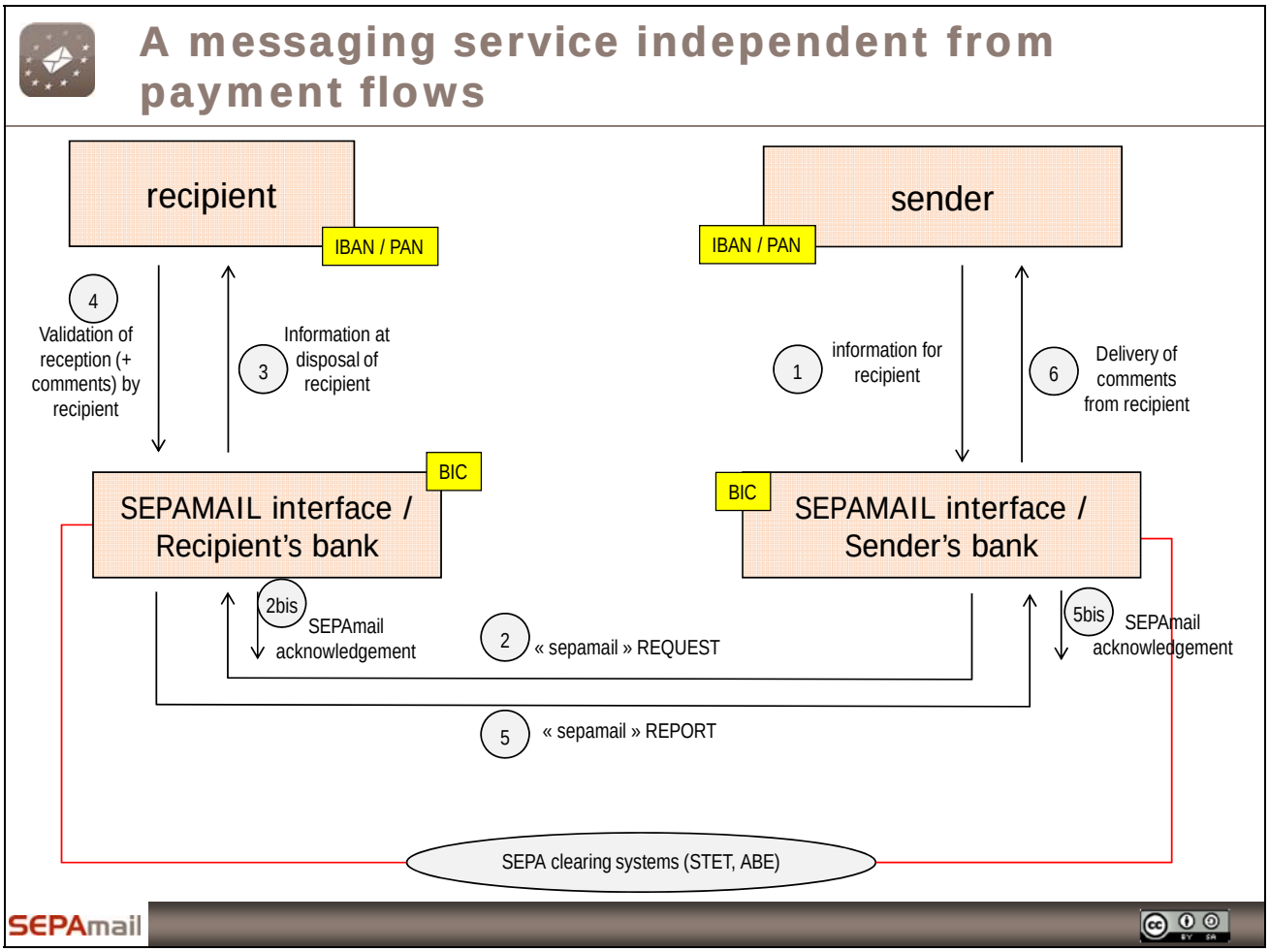
1. The sender initiates an exchange, i.e. it sends information to the attention of the recipient
2. Its messaging service interface authenticates the sender and issues a SEPAmail message. Usually, this first SEPAmail message is called« REQUEST »
    - (2bis) the interface of the recipient receives the data, authenticates the sender's interface, and sends back a message (much more simple) to confirm the receipt of the message, the acknowledgement
3. The recipient's interface makes the data available to the recipient
4. The recipient gets the data and validates if necessary. It also can add comments to its validation
5. The validation of the recipient to its own interface enables the latter to send a message in return, usually called « REPORT », to the sender's interface.
    - (5bis) The sender's interface authenticates the recipient's interface, sends back an acknowledgement message and
6. The sender's interface gives back to the sender the data received (validation and comments, if any).

A standard around ISO 20022 normalisation

The SEPAmail standard has been defined and created based on the strategic aim to provide additional value to economical exchanges. As such, it helps to meet customers' needs around the exchange of payments. Thus, the standard includes concepts used for SEPA payments: credit transfers, direct debits and cards.

- ❑ The identifiers of the recipients and senders comply with the IBAN standards[6] (bank account identification standards) or the PAN standards (card account identification)
- ❑ The identifiers of the messaging service interfaces comply with the BIC[7] standards (identifier of the Payment Services Providers)[8]
- ❑ The standards selected to route the sender's data[9] are the ones from ISO 20022, then enabling
    - An easy articulation with SEPA payments, using ISO 20022 messages,
    - Many existing and well-documented messages
    - The capability to propose new messages to ISO 20022
    - Use of the ISO 20022 dictionary which may speed up the roll out of new services prior to the ISO standardization.

[6] It is really the « IBAN standards » that has been selected and it enables larges capabilities than the strict usage of banking IBAN, as it is done with the QXBAN (IBAN with a QX country code)
[7] It is really the « BIC standards » that has been selected and it enables to use the existing BIC referential but also to define new formats such as the QXBIC (BIC with a QX country code)
[8] The BIN, the banks identifier in the card business is not used as some existing referential enable to get the BIC from the BIN.
[9] To be well distinguished from messaging service standards (routing and security) which are based on the Internet ones (email and web)



In addition to reminding the messaging service identifier standards, the previous diagram demonstrates that, when payments are linked to SEPAmail messages:

- The recipient's interface **is also** the recipient's AS-PSP
- The sender's interface **is also** the sender' AS-PSP
- The SEPAmail exchanges are neither payments nor payment initiations.

A standard compatible with the digital ambition

By wishing to link the messaging service and payments, SEPAmail had to make some impacting choices:

- Promote the « message » mode, which means that the interfaces exchange mutually unitary messages, as performed for emails[10].
- Favour the « email time » while proposing a « quicker » protocol possibility.

[10] By comparison with payments which are mainly batch exchanges between banks.

- The « canonical[11] » mode of the exchanges between the interfaces is performed with responses times similar to emails (SMTP protocol, the Internet emails one). This quality level is compatible with the digital economy requirements while using known and well managed technologies as needed by the volumes challenge. This canonical mode benefits then from the resilience of the email infrastructure.
- The « flash » mode (Web service protocol) enables a higher response time level than the canonical mode provided a more costly infrastructure is implemented.

❑ Mandate a multi-domain architecture enabling the multichannel for senders and recipients

- Mandate of a standardised exchange between the messaging service interfaces
- No direct connection possibility between the sender and the sender's recipient
- This infrastructure brings a real value: refer to next paragraph « an Omni channel system »

❑ Link « structured data » and « human readable data »

- The business data are defined from the ISO 20022 standards in XML formats enabling an automated processing
- The human readable data come from the capability of the standards to route binary flows, mainly in PDF format or images, enabling then the user to retrieve the physical image (electronic paper) but also to manipulate this image, i.e. to store it, to archive it and even to transfer it to a third party, without using specific tools to process XML data.

❑ Enable the creation of many messages which, linked all together and if needed with payments, propose new services (Refer to messages range at the beginning of this chapter).

An Omni channel ecosystem

The SEPAmail architecture, by splitting the various security areas, enables the implementation, by the messaging service customers, of Omni channel approaches:

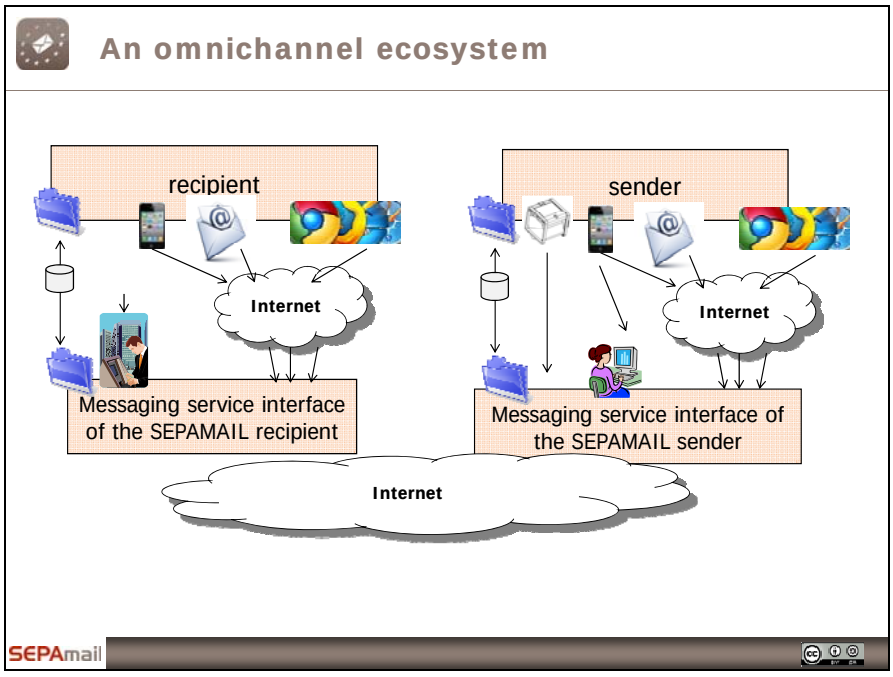
❑ Pure WEB if the sender and the recipient are on the WEB

❑ B2B channels if the sender and the recipient are companies with their own system compatible with SEPAmail messages

❑ Any other mix of a recipient's channel and another sender's channel

❑ The only channel remaining mandatory is an IP link, Internet being preferred, between the 2 interfaces.

[11] Qualifier used by the SEPAmail standards.



To date, several pilots have been performed:

- Messages validation at an ATM
- SEPAmail extension for Thunderbird enabling the processing with a messaging service interface
- E-commerce context, with a purchase on a WEB site and validation in the browser
- Smartphone context, with the use of the SEPAmail standards between the smartphone and the interface
- Messages routing in files mode (EBICS, FTP and other protocols)
- Transmission of messages from the point of sale on secure electronic terminals
- This multiplicity of channels between the sender and its interface on one hand, and between the recipient and its interface on the other hand ensures the access to the system to any entity, including to individuals having a restricted access to Internet.

An extendable implementation

The SEPAmail standard is mainly[12] created and managed by the SEPAmail.eu Company, which also and especially acts as scheme manager. The latter added to its activities some technical services enabling the creation of secure Members network[13] : test tools, unique PKI for the various bank servers, consolidated statistics reporting of the SEPAmail flows.

[12] Mainly as the Creative Commons license of the standards enables any entity to propose a new application. As an example, an application on banking mobility, which means smoothing of the bank domiciliation transfer while changing bank, is currently being finalized by a stakeholder of this business.

[13] Note: the SEPAmail.eu entity does not have access to the flows; they are always bilateral between 2 Members (which means 2 messaging service interfaces having signed the subscription contract with the Scheme Manager).

2. TPPs scope of activities

Current scope of TPPs as of today

The TPP (Third Party Payment Service Providers) are stakeholders proposing to AS-PSP customers some additional services, related to customers' accounts data. Those services already exist for many years in the business area:

- A reference bank getting all the account statements of the banks of a company
- An accounting office getting directly the companies account statements from the AS-PSP without going through the company's Information System
- A processing company having the duty to process the bank domiciliation switch for a new customer, requiring the connection to the bank that is left.

As of today, these services often go through a trilateral contract, bringing some administrative pain but acceptable in a business context. In addition, the data exchanges are secured by the usual securing means restricted to companies.

This type of services is quickly growing as the Internet enables to extend the existing mechanisms to individuals or to small companies, and even to imagine some new ones.

Guiding principles issued by the regulator[14]

A directive (the PSD2) shall organize the TPP legal context. Prior to the adoption of the PSD2 and its transposition in national law, a Working Group of the European Commission proposed the following guiding principles[15] :

1. It should not impede, restrict or obstruct in any way the provision of payment initiation services by any licensed PSP;
2. It should build on state-of-the-art strong customer authentication methods;
3. It should not require any form of agreement, contractual or otherwise, between the TPP and the bank;
4. The Account servicing AS-PSP should be legally required to implement and support the solution;
5. It should be based on open common standards;
6. It should be user-friendly for payment service users (i.e. payers and merchants) and PSP.

[14] First meeting of the Technical workshop on access to the payment accounts by third party payment service providers, on February 18, 2014

[15] Note: the present document doesn't comment these principles but simply highlights how the SEPAmail standards may answer to them.

Overview of existing and potential services

- Collection of account statements of the accounts held by the customer with different banks, in order to aggregate them and provide an enhanced overview to the customer
- Payment initiation via a credit transfer, a card...
- Electronic management and signature of direct debit mandates
- Knowledge of the customer's account balance
- Knowledge of recurring transactions (in the switching context)
- Automation of payment requests and follow-up of the payment receipt directly in the account of a customer, e.g. Gambling site or social network's client, assuming those sites or networks allow economical transactions.
- Additional services related to electronic safe
- Additional security service (customer token usage) or banking data multichannel access services.

In our view, any solution chosen to connect TPPs and AS-PSPs should cover at least all services listed above

3. SEPAmail, a solution for TPPs' access to AS-PSPs

General principles

The TPP, to be regulated by DSP2, is eligible (as any PSP) to become a member of the SEPAmail network

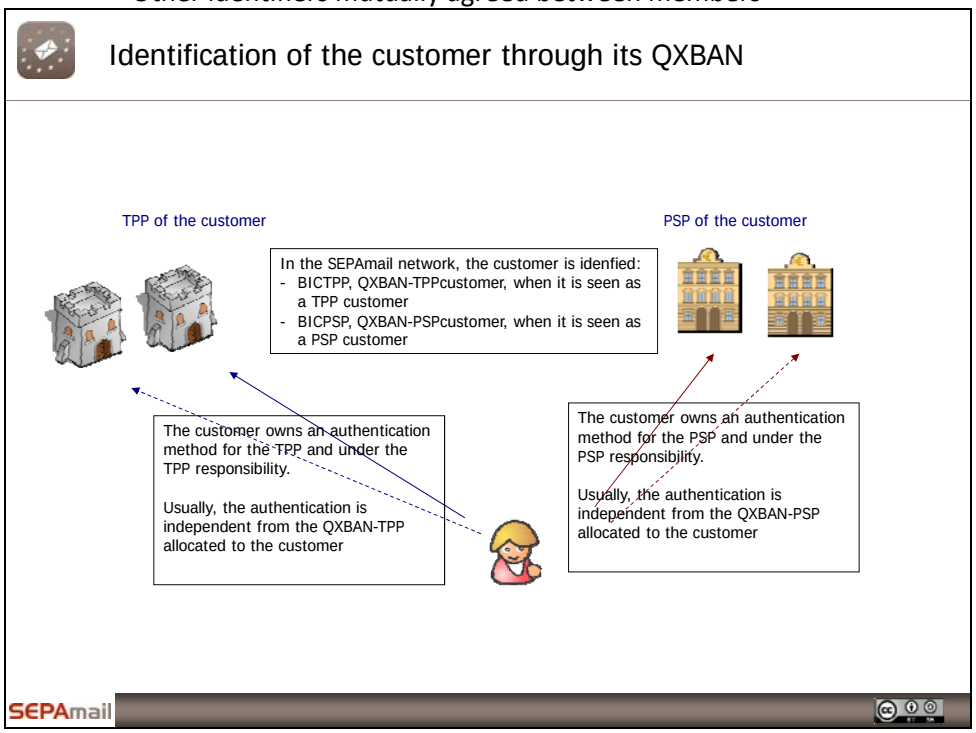
- A TPP might be in relation with all AS-PSPs on the market.
- Thus, in order to benefit from the SEPAmail architecture, the TPP shall be a Member of the Scheme to communicate with all the other PSP members.

The TPP is identified in the network as soon as it become a Scheme Member

- In addition to its subscription, the TPP exchanges with the AS-PSP in compliance with the SEPAmail standards, which enables it to be securely identified by all the other members of the scheme through electronic certificates.
- This answers item 3 of the « technical workshop » which excludes any bilateral agreement between TPPs and AS-PSPs, as well as item 2 relating to strong authentication methods.

The customer's identification is performed through its QXBAN

- The QXBAN is an identifier in form of an IBAN using the QX proprietary code (authorised in the IBAN standards) instead of a country code. It enables an identification system shared all over Europe, without bearing the constraints of IBAN national structures. The QXBAN is directly provided by the AS-PSP or the TPP to its customer.
- Other identifiers may be routed in the SEPAmail messages if needed:
  - Accounts IBAN
  - Cards PAN
  - Other identifiers mutually agreed between members



Authentication of the customers and customers' requests

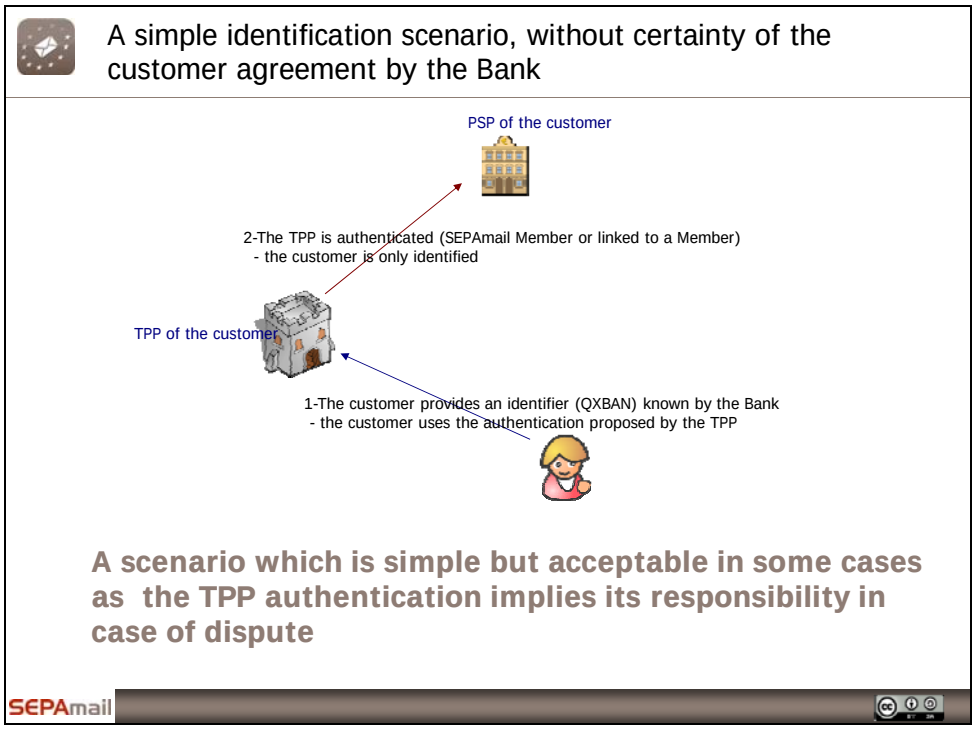
The authentication sensitive point mainly stands at the AS-PSP which will have to perform an action, not directly requested par its customer but by a third party supposed to « have an order » from its customer.

From general concepts, different authentication level may be implemented

- ❑ Simple authentication
- ❑ Strong authentication
- ❑ AS-PSP authentication (level depending on the AS-PSP offer)

All these scenarios avoid any sharing of security credentials, such sharing raising issues for the AS-PSP and the customer.

Simple authentication



- ❑ The customer connects to its TPP using identification/authentication defined by the TPP, activate the proposed service and indicates the QXBAN[16] that identifies it at its AS-PSP
- ❑ The TPP sends a SEPAmail message in accordance with the requested information:
  - FROM: BIC of TPP and QXBAN TPP of the customer
  - TO: BIC of AS-PSP and QXBAN AS-PSP of the customer

[16] Note: the QXBAN includes by structure the BIC of the issuer of the QXBAN and is therefore enough for the TPP to send the message.

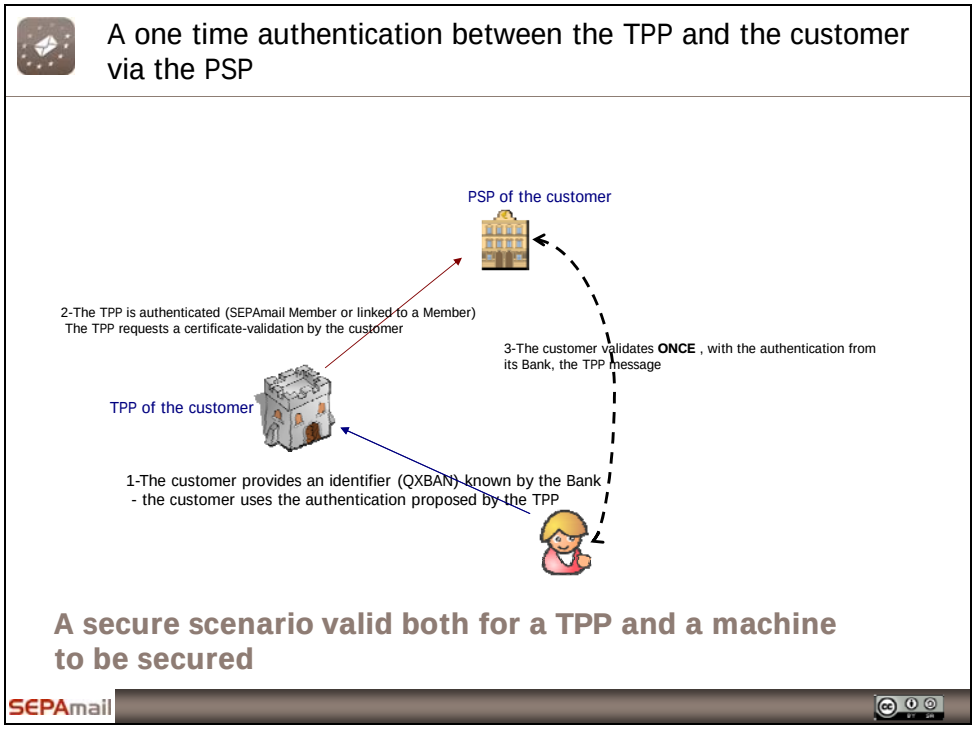
This mode enables the AS-PSP to:

- Identify its customer (using the QXBAN-PSP)
- Authenticate the TPP (Member of the Scheme, BIC of the TPP and certificate of the TPP), which will enable to come back to it in case of a dispute.

Such a scenario seems to be relevant to a sufficient authentication for messages related to information collection (account statements, balance and recurring transactions). This scenario may later involve the creation of a white/black list directly by the customer at its AS-PSP (as it was asked for the credit transfer).

We should note that this scenario, even if simple and easy for the customer, provides a strong security as the TPP is a Member of the Scheme Manager and is liable for its commitments.

One time authentication



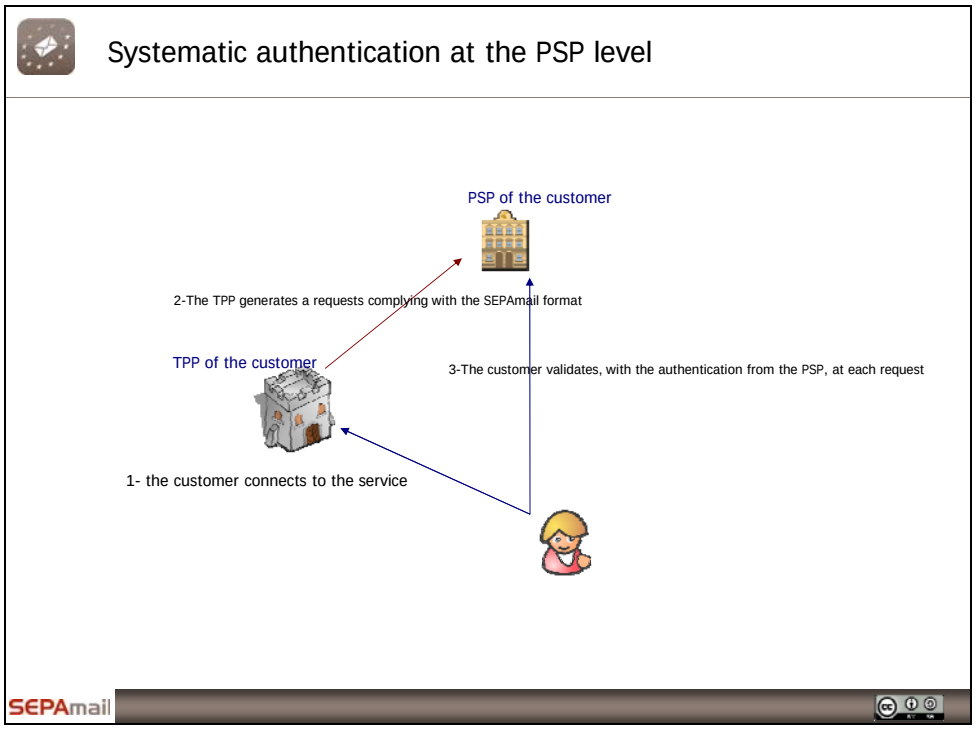
This authentication case includes les principles used for the pilot with the smartphone:

- Before any transaction, the TPP generates some bi-keys and sends on behalf of its customer the public key related to the AS-PSP
- The AS-PSP sets the message including this public key available to its customer which validates this message[17]
- After receipt of the answer, the le TPP may use these bi-keys to sign all the transactions on behalf of its customer regarding the AS-PSP

[17] In order to offer more flexible services management, the customer might indicate in its answer the services that are authorized with the public key: credit transfer process, signature of orders…. Indeed, the authentication is not a purpose on its own but is only useful for the implementation of services.

For the whole process to have a security value, this scenario assumes that the authentication of the customer by its TPP is also strong. It enables to implement additional services to SEPAmail services directly using the customer's public key.

Systematic authentication at the AS-PSP



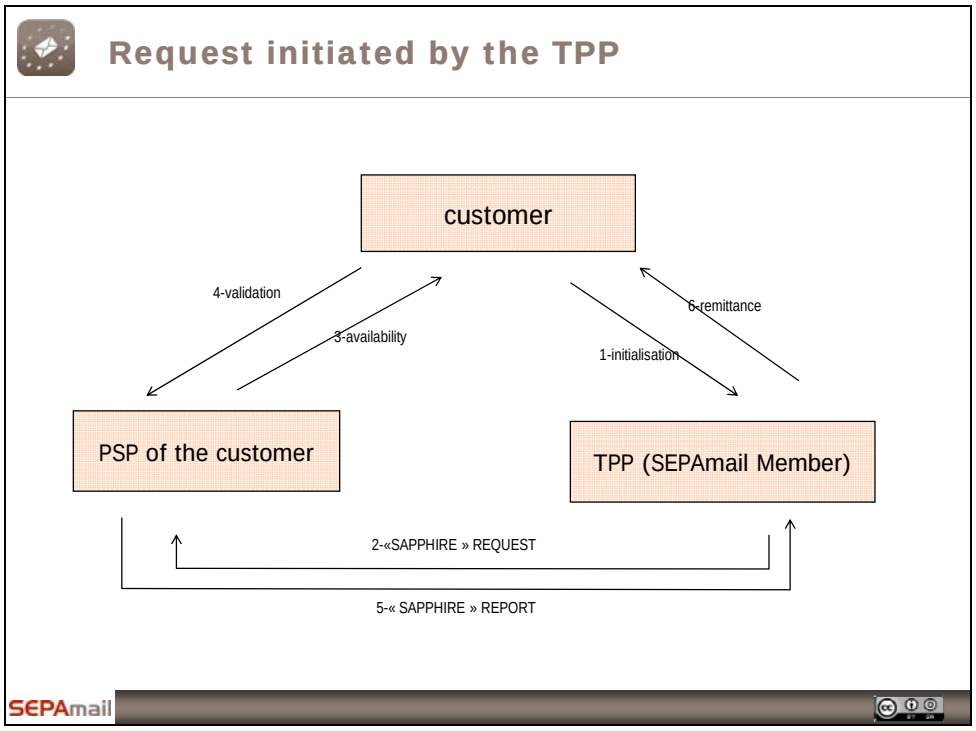
- In this mode, the customer's authentication is no longer implicit or performed once in advance but systematically requested and without any intermediary at the AS-PSP level (customer's request, for instance).
- At each request of the TPP to the AS-PSP, the customer shall then validate
- The benefit of this mode stands in the ease for the TPP which does not need to implement a strong authentication process with the customer: the strong authentication of the customer is done by the AS-PSP.
- This scenario represents an authentication limited to the session.

A highly secured first connection between the TPP and the AS-PSP

A first connection shall be established in order to set-up the authentication mechanisms. Two possibilities exist in SEPAmail:

- Request to the AS-PSP initiated by the TPP
- Request to the AS-PSP initiated by the customer and then transmission to the TPP

Request to the AS-PSP initiated by the TPP



This diagram remains the usual SEPAmail one, prior to transactions, in a context of a unique customer:

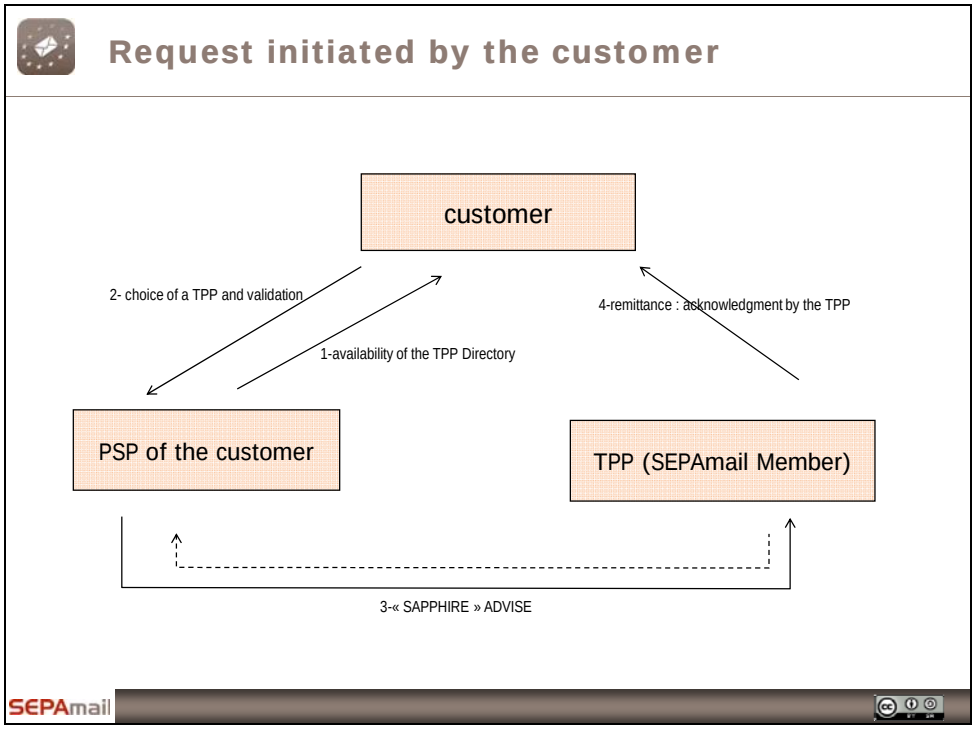
- 1 – Initiation request: the customer connects to the service proposed by the TPP
- 2 – The latter issues a request to the AS-PSP holding the account (or several requests in case of several AS-PSP)
- 3 and 4 – The customer validates at its AS-PSP
- 5 – The AS-PSP sends in the SEPAmail mode the acceptance of the request
- 6 – The TPP may initiate the service

In this context, it is necessary to be able to indicate which future transactions are related to the customer's validation at the AS-PSP (process 4), for instance:

- Acceptance of the RUBIS message (request of a settlement to be paid via a credit transfer)
  - Automatic by the AS-PSP / conditional validation by the customer in addition
  - If automatic, which scope (amount, selection of the e-commerce…)?
- Acceptance of the messages of account statements request for aggregation services (CAMT)
  - Total (which scope (all accounts, all periods, all transactions…) / conditional
- Acceptance of the message of balance information
  - Total / conditional

It will be necessary to define a generic structure enabling a total or conditional acceptance of new messages that could be created depending on the needs and their creation.

Request to the AS-PSP initiated by the customer



- In this case, the customer gets through its AS-PSP a directory of all the TPP
- The customer registers at any TPP it selects with the services and the access level.

Note: a directory already exists for creditors, customers of the AS-PSP, issuing RUBIS service. The creation of directory [18] of all the TPPs, or even of all the PSP as SEPAmail Members, is therefore quite simple.

[18] A referential of all the SEPAmail Members already exists. The directory concept is different as the directory is set available to all the customers, while the referential is for the only use of other Members.

4. RUBIS, a service to request a payment initiation with systematic customer validation

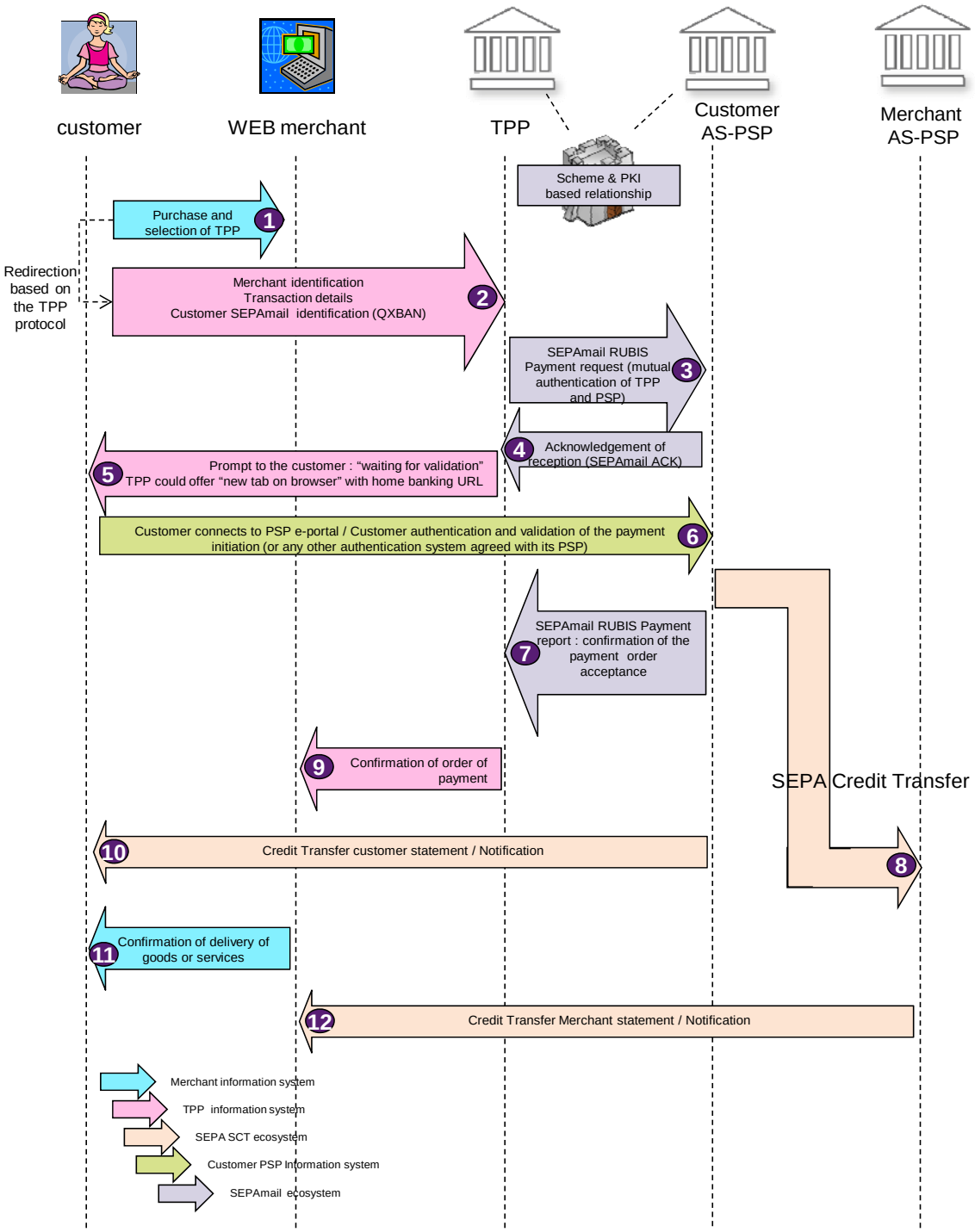
RUBIS is an application enabling to issue a « settlement request » to the debtor's AS-PSP. Through the pilots that were performed, RUBIS demonstrated its capacity in:

- ❑ Sending large volumes of invoices periodically
- ❑ Payment on the Internet (e-commerce)
- ❑ Various possibilities to validate the payment: browser but also smartphone or bank unattended machine (ATM).

Legend of the diagram on the next page

1. Purchase by the customer on the WEB merchant site and selection of the TPP as payment mode
2. Redirection of the customer by the WEB merchant to the TPP with the transaction and payment details, according to the protocol implemented by the TPP and with a transaction number. The customer fills in it QXBAN (except if the WEB merchant already knows it)
    - In terms of banking identifier, the customer is only identified at this stage by its QXBAN. As this identifier is not a sensitive data, it may be stored in the customer's account of the WEB merchant or of the TPP, or simply copied/pasted during the transaction
3. Transmission by the TPP to the AS-PSP holding the account of a SEPAmail-RUBIS message (based on the ISO 20022-pain.013 standards) including the transaction details, the amount and if needed a PDF with a quotation and terms and conditions. The TPP and the AS-PSP authenticate each other with cryptographic methods defined in the standards by using the shared PKI of the scheme manager
4. The AS-PSP send to the TPP an message to acknowledge the receipt of the previous message (also with mutual authentication)
5. On the TPP site, a screen is displayed to request the customer to validate the transaction on its home banking
6. The customer connects to its AS-PSP, authenticates itself (according to the authentication rules defined in its contract) and validates the SEPA credit transfer initiation
7. The SEPA credit transfer initiation is performed by the AS-PSP in accordance with the contract provisions
8. The AS-PSP sends a SEPAmail-RUBIS message (based on the ISO 20022-pain.014 standards) to confirm the acceptance of the payment order given by the customer
    a. Mutual authentication of the AS-PSP and the TPP
9. The TPP may inform the merchant of the payment order acceptance in accordance with its specific protocol with the merchant
10. The SEPA credit transfer finalization is confirmed to the customer by its AS-PSP, or the customer sees the debit on its home banking
11. The merchant may finalize the delivery of goods or services
12. The merchant also receives the notifications or the statements from its own AS-PSP related to the credit transfer receipt. The transaction number provided by the merchant in Step 2 is included in the data of the SEPA credit transfer.

RUBIS enables the TPP to manage the payment initiation service without deleting the validation by the customer and then without interfering with the authentication mode provided by the AS-PSP holding the account to its customer. This mode should be preferred for an occasional purchase. In addition, this mode enables the TPP not to implement a strong authentication method with the debtor customer.



Model involving TPP with direct authentication from customer to its PSP

As SEPAmail is a messaging service standard, it does not plan, in the RUBIS context, the automatic redirection of the customer to the site of its AS-PSP holding the account. The TPP may add this functionality if it wishes to.

However, linked to the RUBIS process, the SAPPHIRE application will enable to complement and simplify the customer experience for regular purchases.

5. SAPPHIRE linked to RUBIS, a service to request payment initiation with validation through the TPP

SAPPHIRE general principles

Sapphire[19] is a protocol enabling to use:

- An electronic device (pc, mobile phone, tablet),
- A software interface out of the « home banking »,
- The Internet network
- A cryptographic mechanism (hardware and possibly software)

It enables the Bank's customer to:

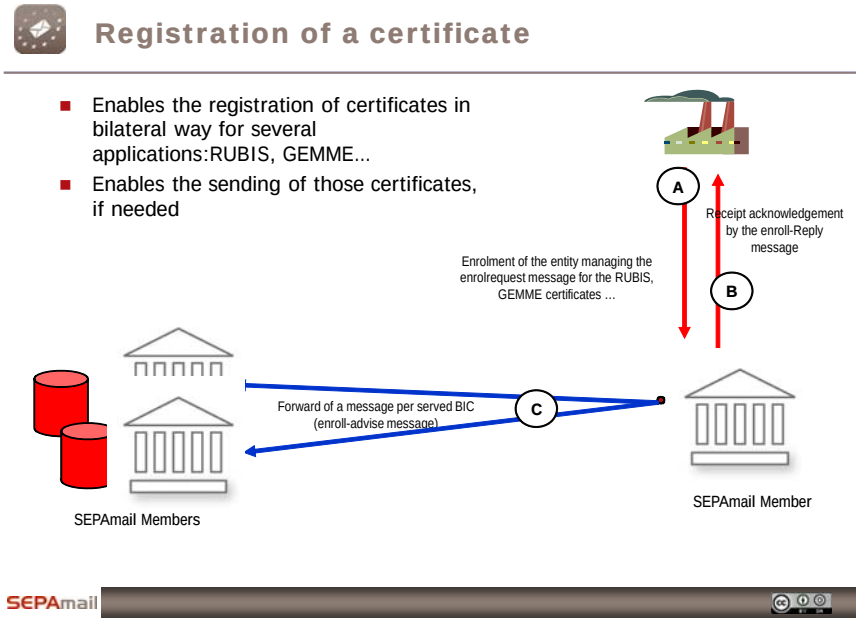
- Authenticate itself on a computer implementing the SEPAmail protocol,
- Electronically sign (several levels) some message of a SEPAmail family to send it to the its bank's SEPAmail interface
- Authenticate itself on any other system of the bank or on a partner system
- Sapphire aims therefore at implementing a managed security of the Internet channel between the user and its bank, with enrolment procedures using the existing secure channels.
- The trust area between a user and its bank is then enriched by a secure authentication plug using:
- The Internet network for the routing
- An application on the user's device
- A certificate enabling an authentication of the user (sapphire authentication) and then of the data sent depending on the required service level (electronic signature, reinforced electronic signature, qualified electronic signature)

The SAPPHIRE messages

There are 3 messages:

- EnrollRequest, enables to request its enrolment to SAPPHIRE and to send a certificate to its bank,
- EnrollReport, enables the SEPAmail Member to answer on the process status of the certificate that was sent,
- EnrollAdvise consists in (i) information message related to the enrolment of a new member, (ii) transmission of its crypto data.

[19] Source « http://documentation.sepamail.eu »



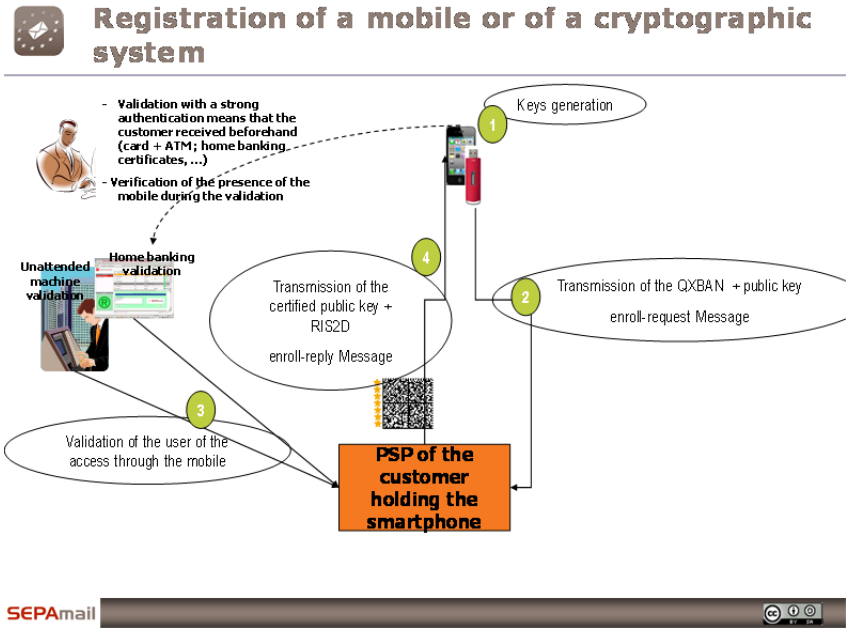
SAPPHIRE has been piloted in 2012

Pilot objective and context

Aiming first at quickly exchanging certificates with business customers, SAPPHIRE has been piloted during 2012 in the smartphones context.

The pilot had planned to use the RUBIS messages to request settlements by using the entire SEPAmail standards between the Member and the Smartphone. The objective was to demonstrate that the SEPAmail protocol could be implemented not only at Members to process thousands of volumes but also on a smartphone to process few transactions.

Security principles with the SECURE messages



The previous diagram includes the principles used to secure the smartphone with the SECURE messages:

- A dedicated application (developed by the AS-PSP and proposing this service), implementing the messages compliant with the SEPAmail standards, is downloaded on the smartphone
- The customer enters its identifier (QXBAN) and the smartphone connects itself to the customer's AS-PSP by sending an « enrollrequest » message with 2 public keys of the Smartphone
- As the AS-PSP already has a secure relation with its customer, it transmits the message through another channel: Remote banking, automatic banking, even a branch
- The customer validates itself this message at the AS-PSP by using the identification method related to the selected channel.
- The AS-PSP may then:
  - either certify the public keys and propose a list of revoked certificates (CRL)[20]. Therefore, the usage of the keys may be extended to other actors (such as administration…)
  - Or more simply store the keys in an internal base for a bilateral usage between the customer and itself.

Once the smartphone keys have been stored, the SEPAmail messages of other applications may be routed and received. As the SEPAmail standard is structured in such a way, additional developments to process a new application are only needed at the data and screens levels. All the security and messaging service softwares are indeed factorized, which means they are used for RUBIS but also for SAPPHIRE and finally for other existing or future applications.

Trust and understanding in addition to security

The pilot also demonstrated that beyond the security mechanisms that were implemented, it is important that the end user understands clearly in which « validation » context it stands. It has been proposed[21] to define 3 levels:

- SAPPHIRE 1: enables the simple authentication
  - With one element: a PIN code on software certificate (what we know) OR the presence of the cryptographic card (what we own)
  - Example: simple consultation of an account or a site without any possibility to modify it
- SAPPHIRE 2: enables the strong authentication
  - With two elements: a PIN code on software certificate (what we know) AND the presence of the cryptographic card (what we own)
  - Example: value added services, access to an account or a site with an action possibility

[20] CRL: revocation list enabling any other stakeholder to check that the key that was sent is valid and not blocked.
[21] SAPPHIRE pilot outcome, BPCE 2012

- ❑ SAPPHIRE 3: enables the individual electronic signature
  - With the 5 conditions of the electronic signature: Real, Unforgeable, One time usage, Not changeable, Non revocable
  - Example: on-line electronic signature or conclusion of contracts

RUBIS with additions from SAPPHIRE

RUBIS may receive additions by using SAPPHIRE. Legend of the diagram on the next page:

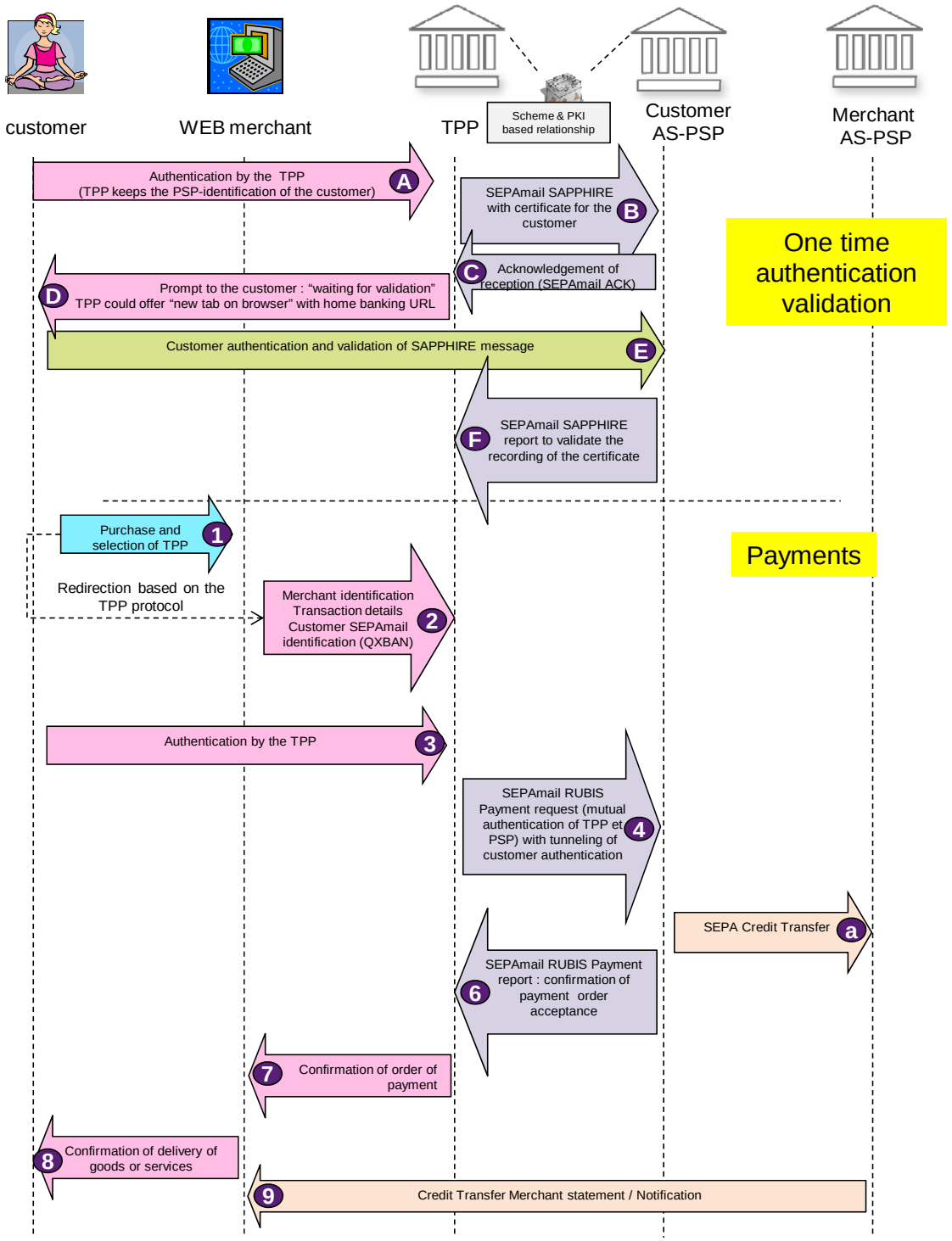
Phase 1: one-time prior authentication validation

A. The customer connects to the TPP for the first time and agrees with it of an authentication method. The TPP generates a bi-key for this customer. The key will not be unlocked unless using the authentication methods defined in A.
B. The TPP sends to the AS-PSP a SAPPHIRE message including the customers 'certificate. The AS-PSP acknowledges. The TPP and the AS-PSP authenticate each other with the cryptographic mechanisms defined in the standards by using the shared PKI of the scheme manager.
C. The AS-PSP sends to the TPP a message to acknowledge the receipt of the previous message (also with mutual authentication)
D. On the TPP site, a screen is displayed to request the customer to validate the transaction on its home banking.
E. The customer connects to the home banking of its AS-PSP holding the account and validates the transaction.
F. Once the validation is performed, the AS-PSP sends to the TPP a message to confirm the registration of the certificate.

Phase 2: subsequent payments

1. Purchase by the customer and selection of the TPP as payment mode
2. Redirection of the customer by the WEB merchant to the TPP with the purchase and payment details, in compliance with the protocol set up by the TPP and with a transaction number
3. Authentication of the customer by the TPP
4. Transmission by the TPP to the TSP holding the account of a SEPAmail-RUBIS message (based on the ISO 20022-pain.013 standards) including the transactions details, the amount and if needed a PDF with a quotation and terms and conditions
   a. The TPP and the AS-PSP authenticate each other with the cryptographic mechanisms defined in the standards by using the shared PKI of the scheme manager
   b. The customer is authenticated through the certificate that was included in advance in the SAPPHIRE message
   c. The TPP validates the payment initiation (as ordered by the customer) on the AS-PSP site
5. The initiation of the SEPA credit transfer is managed by the AS-PSP as defined in the contract provisions
6. The AS-PSP sends a SEPAmail-RUBIS message (based on the ISO 20022-pain.014 standards) to confirm the payment order given by the customer
   a. Mutual authentication of the AS-PSP and the TPP
7. The TPP may inform the merchant of the acceptance by the bank, by using its specific protocol with the merchant

8. The SEPA credit transfer finalization is confirmed to the customer by its AS-PSP, or the customer sees the debit on its home banking
9. The merchant may finalize the delivery of goods or services
10. The merchant also receives the notifications or the statements from its own AS-PSP related to the credit transfer receipt. The transaction number provided by the merchant in Step 2 is included in the data of the SEPA credit transfer.



Model involving TPP with direct authentication by the customer on the TPP

6. Conclusion

SEPAmail does offer a solution to connect TPP and AS-PSP while granting a high security level as currently foreseen by the European Authorities (PSD2). We demonstrate during the past 5 years that the approach is realistic and could be achieved at reasonable costs with incremental steps. Furthermore, the migration towards the SEPAmail infrastructure could be done form scratch (as France is currently working on) or by interoperability with existing structures or schemes (as we do with the SEPA Schemes).

Nevertheless, we believe that the issues raised by the TPP are one emerging part of the iceberg of the digital economy. If the short term could be solved by simple authentication solutions and limited to 2 new services (initiation of payments and account access), the real ambition should be to offer full digital services as anticipated by the Lisbon Agenda and Europe 2020.

SEPAmail has been designed to offer to the all the actors of the European economy a digital secure infrastructure, which could be enhanced by new messages. Effectively, the SEPAmail message structure enables to securely convey any type of information, XML for machines and Human readable PDF, thus allowing its use by any kind of industry. Indeed, it is possible to create others SEPAmail Schemes for usage in areas others than the payments one.