Realising SEPA Benefits

Corporate Requirements and Key Elements of the Business Solution

This document is a White Paper drafted by an ad-hoc committee of TWIST Process Innovations Limited. This committee is tasked to provide input to the EU Commission on matters regarding SEPA Incentives. The Commission's SEPA Incentives project explores ways to support, underpin and enhance the self-regulatory activities of industry regarding the realisation of the Single Euro Payment Area (SEPA).

The White Paper is designed to feed the debate on how payment services should be developed to meet the needs of corporates, when transferring funds and the underlying data to counterparties in particular within European countries and across Europe. The many contributors to this paper are very interested to obtain feedback as well as further input and suggestions, aiming for this paper to be a live, "open source" document that helps shaping the debate around SEPA and the solutions for its implementation.

As the paper is aimed at those who are involved in the discussion about the Single Euro Payment Area (SEPA) from a business perspective, it has been kept at an appropriate business and functional rather than technical level. Nevertheless, it proposes a set of key components for a business solution that is fully workable, and can be further detailed when required. Although the initial focus of SEPA is on the euro payments, the model is equally valid and extensible to other currencies which may be included in due course.

White Paper
TWIST Innovations Centre

Version 1.0 - London, May 15th, 2006
Feedback and input on this White Paper are welcomed. Please provide comments to
tom.buschman@twiststandards.org and pguldentops@twiststandards.org

Contents

1 Introduction 3
2 An EU Single Market in Payments – the New Legal Framework 3
3 Current Position – A Gap Between Vision and Execution? 5
4 Corporate Requirements – Realising the True Benefits of SEPA 7
5 Key Elements of the Business Solution 8
5.1 Choice of Entry Point 8
5.2 Standardised Access and Predictable Results 9
5.3 Portability of Bank Account 10
5.4 Open Architecture 10
5.5 Central Bank and Regulatory Control 12
5.6 Governance of Payment Services Provision 12
5.7 Identity and Attribute Management 13
5.8 Cost, Transparency and Transaction Reporting 13
5.9 Implementation and Migration 14
5.10 Operational and Non-Functional 15
6 A Potential Systems Architecture 15
6.1 Summary Architecture 15
6.2 Trust Model 16
6.3 Liability Management 18
6.4 Enriched Message Standards 18
6.5 Operational Services 19
7 Impact on the European Payments Market 19
8 Conclusion - Key Enablers for the True SEPA Vision 20
Appendix 1 – The Regulatory Context for this White Paper 22

1 Introduction

The White Paper is designed to feed the debate on how payment services should be developed to meet the needs of corporates, when transferring funds and the underlying data to counterparties in particular within European countries and across Europe. These corporates form a relevant group of stakeholders for SEPA given that changes to payment processes are likely to cause a noticeable impact to business processes and complex system infrastructures of corporate users. Further, in most European countries banks generate more revenues from corporates, which include merchants, for their payment services than from consumers. This means that changes in payment services and the associated costs are likely to have a higher impact on corporate users than on consumers.

As the paper is aimed at those who are involved in the discussion about the Single Euro Payment Area (SEPA) from a business perspective, it has been kept at an appropriate business and functional rather than technical level. Nevertheless, it recommends a business solution that is fully workable and can be further detailed when required. Although the initial focus of SEPA is on euro payments, the model is equally valid and extensible to other currencies inside and outside of Europe which may be included in due course.

This paper represents the views of an ad-hoc working group of TWIST Process Innovations Ltd, and reflects discussions with the European Association of Corporate Treasurers (EACT). Contributions have been provided by representatives from corporations, banks, and many service providers of the banking sector in and outside of Europe.

After outlining the general benefits of SEPA and the related EU Payments Directive, this paper focuses on corporate requirements for payments processing that would extract additional benefits and value from SEPA and ensure its adoption by 2010. It presents the key elements for a corporate driven business solution and a potential systems architecture.

2 An EU Single Market in Payments – the Payments Directive

Pan-European commerce should flow as freely as electricity. But it does not yet because of complex paper trails and incomplete automation. Modern, straight through financial processing of purchasing, ordering, invoicing, payments and financing is frustrated by paper-based processes and disjointed attempts at automation. As part of the EU's modernisation agenda, we can now create a European environment where commerce can move as easily as electricity through integrated systems using common standards. Once these standards are in place, doing business anywhere in Europe will be as easy for any company, large or small, as throwing a switch.

Each commercial transaction includes a payment to pay for products and services delivered. A well-designed payment process enables commerce to flow efficiently, both within a country's boundaries and when crossing borders. The European Commission and the European Central Bank have embarked on a laudable mission to harmonise electronic payment processing in Europe based on user requirements. Given the major benefits to consumers, merchants, payments providers and the European Single Market, we welcome the work of the Commission, in conjunction with the European Central Bank and the European finance sector, to introduce a Payments Directive, or New Legal Framework, which will clear away the legal barriers blocking the Single Euro Payment Area (SEPA).

Background

- To date there exists no common legal framework for non-cash payments between EU Member States. Thus effectively the Euro common currency does not 'exist' electronically across the Eurozone, i.e. in the same way the US$ works across all federal States in the USA, and the £ sterling across all constituent countries of the United Kingdom.
- The New Legal Framework proposed by the Commission on 1 December 2005 will harmonise the rules for electronic payments between EU Member States, legally enabling a Single Market for Payments across the EU (for both the Single Euro Payments Area SEPA and national currencies).

- The SEPA project of the European Central Bank and the banks' European Payments Council will also allow economies of scale and scope across the EU's community of financial services providers
- The New Legal Framework will facilitate electronic payments between Member States so that these are as easy, cheap and secure as they are already within Member States' national frontiers. This will help all EU consumers and EU, SMEs to participate fully in the benefits of the Single Market and not just the big international enterprises.
- These across-the-board benefits, to consumers, merchants, banks and the Single Market are so major that timely implementation by the target date of 2010 is imperative.

Why an EU Single Market in Payments:

- An efficient EU-wide Payments Market is fundamental to make the EU Single Market function efficiently. It is also a key to the Lisbon Agenda to create growth and jobs.
- Studies estimate that the present, fragmented EU payments system absorbs between 2.5% and 3.0% of EU GDP. The equivalent figure in the most advanced Member States is only 1%. Freeing up to 2% of EU GDP for alternative investment and demand generation would provide a substantial boost to EU productivity and employment.
- The current regime of 25 national payments markets, with divergent legal conditions and widely differing prices and speed of delivery, denies EU citizens efficiencies to be gained through a consolidated payments processing system. It obliges excessive use of cash and cheques, and sustains differences between national payment infrastructures, price and service levels. Reform will yield administrative savings and a seamless payment experience for consumers and merchants across the EU.
- SMEs in particular will benefit as their banks import best practices from across the EU, with cross-border payments made as easy and cheap as those within their home country.
- The Commission's timetable for the New Legal Framework calls for the adoption of the Directive as soon as possible and by 2007 at the latest. This is essential so the national legal frameworks necessary for these new financial services are in place by the European Central Bank's target date of January 1, 2008.

Benefits of the EU Single Market for Payments - to Consumers and Merchants

- Payments services cannot work efficiently without legal certainty. They are built on the trust of users. This trust itself depends on a clear legal environment.
- Harmonising this legal environment across the EU will stimulate competitive opportunity to reduce prices for consumers and merchants and to streamline the internal processes of payments service providers.
- Consumer Protection: whatever the payment method (card, direct debit, credit transfer etc), consumers and merchants will enjoy one consistent protection regime and legal certainty irrespective of the payment source.
- Rapid and cheap Payment Transfers - particularly important to SMEs is that merchants will receive payments made in the same currency by the end of the next day at the latest. The New Legal Framework establishes a single set of rules. This will encourage EU-wide competition among payments services providers promoting new process efficiencies and market entry by new entrants such as money remitters and supermarkets.
- As pointed out recently by the EU retail and wholesale trade sector representative body, Eurocommerce (http://www.eurocommerce.be/index.jsp?ptp=tDetail.jsp&MenuID=null&pci=2&pti=2&psk=02&pww=OK) currently there are substantial differences in fees for payments services across Europe (up to 9 times higher for credit cards and 20! Times higher for debit cards). This is hard to defend for essentially the same service to the same economic community.
- The New Legal Framework is essential to supply chain automation across the EU. To quote Commissioner McCreevy's speech of 21 March 2006, "today the payments system is limping behind the physical distribution system. ..... Today it can take 5 or more days for a euro payment to be made from one Member State to another, whereas the lorry full of goods has already arrived....days earlier! "

- Enabled by the New Legal Framework, SEPA will permit fully automated payment processing, with transparent and efficient e-invoicing and payments, to standards consistent across the EU, easing SMEs' access to working capital financing at lowest cost.

Benefits of the EU Single Market for Payments - to Payments Providers

- Overall, payments providers stand to gain provided they use the New Legal Framework from the start with a clear vision of its potential, and the appropriate standards for a Single Market for Payments. Those with pan-EU activity and aspirations stand to benefit differently from those with a fixed local focus, such as perhaps savings banks.
- Payments market integration will strengthen market competitiveness of the financial sector and offer a unique opportunity for payments providers to reduce their operational costs.
- Already, value-added services linked to e-invoicing have become a valuable source of profitable business to banks in some Member States, at relatively minor additional cost in process design.
- Another opportunity is that cash payments are relatively expensive to process. If the use of debit cards achieved in the three Member States with the lowest share of cash payments were to be extended to all Member States, banks are estimated to save Euro 5.3 billion per annum.
- Product standardisation and consolidation of payment infrastructures will maximise economies of scale. For example, if unit cost overall were cut to 20% above the current best practice in the EU, this would generate Euro 10 billion of additional profit overall.
- If the cost of producing payments services overall could be reduced to the levels of the most efficient Member States, e.g. from over Euro 1 down to 20 cents per transfer, massive savings could be achieved.

Costs of Implementing the New Legal Framework for a Single Market in Payments

- The imperative to achieve the benefits for businesses and consumers means that greater emphasis has been placed on SEPA completion than on the attendant costs.
- The Commission has studied these and made suggestions how they might be mitigated, not least by using SEPA to reposition cash and cheques and by implementing e-invoicing.
- There are also costs associated with the development of e-invoicing. But a crucial insight from the experience of Member States where banks developed profitable value-add services linked to e-invoicing, is that the additional cost is relatively minor provided a clear vision of the potential of e-invoicing and the appropriate standards are applied from the start.
- This vision is essential too, to avoid the risk that in spite of the New Legal Framework, SEPA becomes no more than an additional system for cross-border payment rather than the enabling system to fulfil the promise of the Single Market.

3 Current Position – A Gap Between Vision and Execution?

Progress with Payments Directive

The EU Commission treats the Payments Directive with high priority. When speaking at a dinner early May 2006 with the European Central Bank and high level representatives from the banking sector, EU Commissioner McCreevy commented that “Quite simply, no Payments Directive, no SEPA. We are working hard in the Council and Parliament to secure its rapid adoption. I am pleased to say that these discussions have started in a constructive spirit. Although much remains to be done, we are hopeful that agreement can be reached by the autumn.” [1]

Represented via organisations like the UK’s ACT and the EACT, corporates generally welcome the Commission’s proposed Payments Directive in how it sets a framework for standardised rights and obligations for providers and users of payment services in the EU. The Directive has a strong emphasis

[1] Statement by C. McCreevy for the 4th of May dinner with the ECB and high-level representatives of the banking sector

on a high level of consumer protection. This includes mandatory/default execution time of one day for payments (for payments below EUR 50k), the liability of the payment provider for correct execution, and a guarantee of full and timely payment. The stated aim by the Commission is to make cross-border payments - by credit card, debit card, electronic bank transfer, direct debit or any other means - "as easy, cheap and secure as 'national' payments within one Member State".

Corporates feel that the Directive indeed sets the scene for the realisation of most, if not all, corporate requirements for payment processing. However, as stated by the EACT, corporates would welcome if the NLF would also apply to payments over EU 50,000, and would welcome inclusion of corporates in the treatment of responsibilities by payment service providers in the case of non-authorised transactions.[2] This support for the Directive as legal context for payment processing in Europe does not mean automatically however that corporates would embrace pro-actively any operational solution for harmonised payment processing offered to them.

Implementation of SEPA

Through the European Payment Council (EPC), the banks are working on implementing SEPA. The EPC finalised in March 2006 a set of European payment schemes for core and basic services covering direct debits and credit transfers, a framework for card transactions and a framework for cash to be used by the banking industry to offer their customers in 2008.

Commenting on the EPC's work, McCreevy stated at the same dinner in May 2006 that these schemes and the card framework provide a stable platform for the launch of the first SEPA products in 2008. However, he pointed out a number of concerns. One of these concerns is with the intended mass migration in Europe to SEPA products by end 2010: "The Commission fully supports a self-regulatory, market driven process for SEPA. The current EPC rules are sufficient for the launch of SEPA products in 2008, but in the longer term they need to be sufficiently attractive so that the market will use them. If not, we will have no migration, no integrated payments market, and no scale efficiencies. All we will have done is created an expensive white elephant for cross-border payments. So how we can achieve successful mass migration to SEPA products by end 2010?"

These comments from McCreevy are not the only publicly stated concerns about the pace as well as user-focus of the SEPA implementation as planned by the EPC. On February 13th 2006, the European Commission published a "Consultative paper on SEPA Incentives"[3], exploring ways to support, underpin and enhance the self-regulatory activities of industry regarding the realisation of the Single Euro Payment Area (SEPA). The paper mentions that "[...] the Commission largely shares the overall objectives and market driven process of the EPC. However, it also examines the gaps between this vision and the EPC work. […] The Commission is afraid that products based on the schemes as currently developed may not be persuasive to all end users."[4]

Expressing the Commission's vision on the self-regulatory process, the same paper concludes that "[…] for competition in network industries to succeed and deliver the expected huge savings for the EU economy three basic criteria must be met[5]:

a) there must be common standards which are set in an open, transparent and accountable process which can also revise or adapt them in future as necessary;

b) there must be infrastructures available that are collectively characterised by full technical and commercial interoperability, and

c) there must be transparent cost-based pricing to encourage the use of efficient payment instruments to the detriment of expensive payment instruments.

The Commission does not see the move to SEPA as a one-off process. It comments on the future orientation of SEPA schemes, stating that "Finally, SEPA generates a lot of momentum to improve

[2] As Association of Corporate Treasurers (ACT) comments on the draft Payments Directive Com(2005) 603 Final Dated 1.12.2005
[3] This paper can be downloaded from the European Commission website under: http://europa.eu.int/comm/internal_market/payments/sepa/index_en.htm
[4] Page 5 of SEPA Incentives paper, European Commission
[5] Page 8 of SEPA Incentives paper, European Commission

payment systems. It opens a great window of opportunity for a technology leap. We should use this opportunity, be visionary and look beyond the borders of the traditional payment services sector. […]"[6]

New angle harnessing current capabilities

The EU Commission has a strong preference for market forces to result in the definition and adoption of operational market solutions. Within this context the ideal drive for a market based solution without regulatory intervention would be corporate acceptance of new services offered by payment service providers. The logic would be that these services are based on clarified corporate requirements for the business solution for payment services, adhering to open market practices and ensuring these requirements complement or reinforce requirements of consumer user of payment services.

Building on the work done within TWIST, the authors believe there is an opportunity to approach the problem from a new angle, harnessing the capabilities of current ACH and Bank systems in a way that will create drivers for improved efficiency, service innovation and transparency in the European cross border payments market. Such an approach does not invalidate the work of the EPC which covers inter-bank arrangements and contractual and technical arrangements to facilitate the development of European credit transfer and direct debit products by banks. The suggestions made in this paper can be regarded as complementary to the EPC's Rulebooks.

In essence we believe that, consistent both with the recitals and articles of EU Regulation 2560/2001 and with public statements of both the EU Commission and the European Central Bank regarding SEPA, the full Payer-to-Payee requirements should drive the SEPA work. This will ensure that the planned pan-European payment instruments are able to underpin free efficient trade and a market for service offering by banks to their clientele.

The EPC Rulebooks have a strong focus on Customer-to-Bank or ACH-to-Bank processing, and pay limited attention to the full requirements of the Payer-to-Payee transaction. There is, therefore, a need for a complementary effort to address the areas not within the scope of the EPC's effort, if the full benefits envisaged and enabled by SEPA are to be realised.

4 Corporate Requirements – Realising the True Benefits of SEPA

Corporates can be expected to fully agree with the NLF's objective to establish a modern and comprehensive set of rules applicable to all payment services in the European Union. The removal of legal obstacles to a Single Payment Area should allow competition on equal terms, adequate protection of payment service users, security of payments, increase the efficiency of payment systems and should guarantee legal certainty for all relevant parties in the payment process. Yet whether operational solutions offered in the context of SEPA will be accepted as a replacement for existing cross border as well as national payment services will depend on the value these services provide compared with existing services and whether the benefits outweigh the costs and risks of migration. Hence it will be essential to focus on corporate requirements for payment services as a starting point for the specification of these new SEPA payment services.

Corporate users of payment services have a range of high-level requirements which can be summarised as follows:

1. To have free choice to access payment services available in the market, for all payments, whether domestic or cross-border, throughout the EU. This means that corporates should be able to change payment services providers with minimum cost to themselves or their counterparties.
2. To implement open standards that enable end-to-end, cross border supply chain automation within the EU, between large and small organisations, including government agencies. This should include the potential for ensuring that there is a clear linkage between the payment and underlying logistical information such as product identifiers and tracking information (e.g., RFID identifiers included in invoices). Implicit in this requirement is a need for a robust liability model.

[6] Page 20, SEPA Incentives paper, European Commission

3. To implement automated controls and to be able to audit these efficiently to meet regulatory requirements such as Bank Reporting, Sarbanes-Oxley (SoX) and Anti Money Laundering (AML) in a standardised manner in multiple countries.
4. To have ownership of their own identities and attributes, and be able to utilise these identities and attributes in all their transactions and information exchanges across the EU. This should enable corporates to exercise clear management control of their own data in accordance with EU Law, and should enable efficient solutions to "Know Your Customer" requirements.
5. To reflect the Commission's guidelines and deliver lower cost, transparent pricing and billing, coupled with more efficient and immediately reconcilable transaction reporting services.
6. As these services are brought to market corporates need to be able to migrate their existing systems to the new standards without significant effort beyond testing.

To deliver against these requirements a set of core architectural components are needed:

1. A Trust and Identity Management model that is recognised and accepted by all parties, and is under the control of the identity owner. This would also need to include new ways to manage and confirm the authorisation levels required for transactions and how these are made available to relying parties for confirmation.
2. Networking protocols and message adapters based on open standards, that provide a generic connection between corporates, banks and ACHs, to reduce the level of change that corporates, banks and ACH's need to undergo. These generic connections are key enablers for the offering of complementary, value adding services to corporate users of payment services.
3. A solution for managing the settlement limits, liabilities and authorisation levels of the individual parties in real-time to enable multiple banks and ACH's to process payments without the need for a pre-existing bilateral contractual relationship.
4. Standardised payment initiation messages which can be directed to, and accepted by any bank or ACH and which can carry the underlying supply chain information for delivery through a wide range of mechanisms.
5. A set of operational services to enable the administration and charging arrangements to operate effectively in an open environment.

Finally, we would like to point out that the proposed architecture also helps to deliver the environment aimed at by the Markets in Financial Instruments Directive (MiFID). The Trust and Identity Management Model discussed above, is one prime example of a solutions component that is relevant for both SEPA and MiFID. Indeed, operational excellence and market transparency will put pressure on trading parties to manage the risks associated with trading with counterparties, in real-time.

5 Key Elements of the Business Solution

5.1 Choice of Entry Point

Currently corporates have a limited set of options when submitting payment files for clearing and settlement:

- Submit individual payments or files of payments to their bank which then routes them for settlement through a variety of mechanisms, such as a local clearing system or ACH, SWIFT etc. In some cases banks route payments through their own internal network or through an extended correspondent bank network to local clearing systems in the country of the beneficiary account.
- In some countries it is possible to submit payment files and individual payments direct to an ACH under the sponsorship of a bank, and these payments are then sorted and settled appropriately back to individual banks. However, this is normally only able to handle payments in that one country.

- In some countries, the customer can designate the payment service to be used. For example, the UK, US and Japan are examples of markets where already today for domestic payments, the customer can designate the payment service (e.g., CHAPS versus BACS, CHIPS versus Fed).

The overriding control of these services is centred on a single bank, or small number of banks with which the corporate has a relationship. This situation provides limited possibilities for portability of a corporates' payments business. If a corporate maintains a large number of bank relationships, a major cost in itself, it also has to be able to submit transaction requests in a very wide range of formats via differing systems requiring bespoke authentication /authorisation protocols.

This situation also hampers the ability for new service providers to enter the market in case the customer interfaces and embedded security and connectivity protocols are proprietary to the bank or the processor it has engaged. The threshold for new service providers to try to connect to these customers can then be too high.

To create a more competitive market place for payments and remove a number of steps in the process, corporates should be able to access the payment chain at the most cost effective point. Today's options might therefore be extended to include:

- The ability for a corporate to send files of payments to the most appropriate ACH to process these payments, irrespective of the country of domicile of the ACH, where these payments are to be enacted with a single debit or credit being passed back to the corporate's main account. Where there are multiple clearing and settlement choices for the SEPA region after its implementation, then effectively the customer could choose on price and/or functionality plus performance. For example, assuming there will be market demand for real-time execution and authentication of payment transactions, this freedom of choice of entry point would enable ACHs or other payment service providers to offer such real-time services to the European market.
- The ability to send individual or files of payments to a single bank which may hold the accounts for all the payments. This might be particularly appropriate for large volume payers such as government agencies, pension/insurance companies or utility companies. Don't follow what is meant here?
- The ability to make use of services that third party intermediaries may develop, to break down large files, sort the payments, and distribute them for the corporate to the most effective ACH or bank for the payments concerned, based on execution parameters, such as least cost or fastest execution.

In essence this would mean that a corporate could decide to separate some of the processing currently performed by its bank(s) and either do it itself, or outsource to another service provider, thereby breaking down payment files into blocks that can be processed in the most cost effective way and / or in a manner with minimised operational risk. Such flexibility may be welcomed by those banks who prefer to have the option to pass certain operational risks and / or costs of payment processing to ACHs or other service providers.

5.2 Standardised Access and Predictable Results

In order to truly enjoy the ability to switch to the best choice service provider, a customer should be able to send transactions to any SEPA bank and get the same, predictable business result.

In support of this, all banks in the SEPA area should therefore:

- provide services with the same standardised message standards
- use the same standardised customer interface and network standards
- use the same standardised customer identification and message encryption standards
- be able to deliver payments and related data to any account holding bank within the SEPA.

Given a certain service level agreement with its chosen provider, corporates should experience no differences in the outcome, whether the SEPA payment services are provided directly by the bank's own IT services, by an outsourced IT company or by an outsourced ACH company. The bank's choice of delivery mechanism will of course impinge on matters such as the cost effectiveness and service quality it can offer to the corporate.

As part of the bank's ability to outsource to an ACH the fulfilment of customer payment instructions, the customer would potentially need direct access to such ACH's, using the same standards as those detailed above. However, the contractual relationships will likely remain between the bank and the corporate customer in this case as long as the bank offers a value adding service in being the contractor / aggregator for clients.

Since it is unlikely that any service provider will be able to reach 100% of the accounts directly, throughout the 25 affected countries, this implies a requirement for banks and ACHs to develop an inter-operable solution capable of delivering payments and accompanying data to those destinations not within their direct reach.

5.3 Portability of Bank Account

In addition to the standardised access and predictability of service provision, a second key enabler for corporates to gain the ability to switch to the best choice service provider, would be to make bank accounts portable within the SEPA. This would mean that a participant could switch their account to a new payment service provider, without having to undergo the mammoth administrative exercise generally entailed today, where a new account is opened and all the related payment, direct debit, collection and invoicing information has to be updated and communicated to the relevant parties. In fact instruction mandates, such as direct debits, wages/salary or benefits payments and so forth, applied on a portable account would simply transfer to the new service provider. This requirement is analogous to that in the world of telephony, where a customer wishing to change his mobile service provider can simply transfer his mobile number to the new provider.

The work done by the New York Clearing House on the Universal Payment Identification Codes (UPICs) provides an example of how some of this can be implemented. This scheme is based on reference identifiers that point to existing bank accounts for the routing of payment instructions, thus enabling portability of account identifiers. This scheme could be introduced in Europe with the improvement of applying account number / name structures that are similar to the structures used for internet addresses. [7] This approach enables consistency and hence interoperability with other business, document and individual identifiers which in general are becoming more and more based on general, user defined requirements instead of individual, provider-based specifications (see further section 4.7).

5.4 Open Architecture

If we are to realize the 'choice of entry point' mentioned above, we will require an infrastructure capable of supporting an efficient operation over a wide range of operating postures and service solutions. To avoid serious operational risk, such an infrastructure must represent no more than an evolutionary change from today's systems, while being positioned to cater for the anticipated high rates of innovation and evolution. Critically, under the requirements of SEPA, none of the participants has the option to wait. Whilst the benefits of the architecture described here will be crucial to corporates, it also provides immediate and consequential benefits throughout the Community, and therefore deserves special attention.

[7] For more information on UPIC, see www.upic.com

In this environment an open architecture is best suited to meet the needs of the Community and all of the participants. The essential characteristic of an open architecture is that all candidate users have access to the specifications and therefore a choice in technology solution. Because multiple open architectures may evolve, we seek open architectures having broad *extensibility* and exhibiting robust *composability*:

- *Extensibility* is a characteristic of the architecture endowing other users with the ability to describe extensions to the architecture, which when deployed will support the introduction of new services that are interoperable on a network with both standard and enhanced implementations. This means that service providers who wish to offer their customers a richer set of services can do so while inter-operating with those who support only more basic services. An example of this would be where a provider chooses to offer a service to execute a payment to deliver value to the beneficiary on a specified date. This requires an extension to the current IST Payment Kernel message set, and some banks would be currently unable to support the service. Nevertheless in the extensible architecture, a bank which is willing and able to do so can offer the service while still utilising the standard message elements.

- *Composability* describes a characteristic of the architecture wherein its layers, adapters, and features may be selected independently of each other, offering the ability for other users to substitute or interpose their own layers or features while protecting other users from change. This means that individual service providers may provide their own branded services through standard mechanisms, while the customer still has the option to switch service provider if required without a major upheaval.

By seeking extensibility and composability we gain the strong likelihood of high levels of interoperability among implementations of each such architecture, across the EU, while allowing further innovation to proceed.

In order to achieve the objective of continuity of interoperability while providing for broad extensibility and robust composibility, the development of the architecture needs to be managed and controlled within one or more coordinating, provider independent, standards development organizations involving all central constituencies. Implementations of these architectures must exhibit conformance to comprehensive interoperability requirements.

Our vision of such architecture includes the need for transport and message formats as well as identity services. These are seen as integral at each stage, layer, extension, and service, and include capabilities extending from the transport and message formats to a general top-level framework suitable for identity-enabling other general architectures and services (e.g., mobile).

Together these requirements will support the integration of solutions across a broad range of users over many successive timeframes. Such architectures will facilitate continued use and improvement of pre-existing infrastructure and solutions, such as PKI, directories, attributes, and services interfaces—thus leveraging existing investments while enabling early change. Architectures meeting these requirements will allow corporates to evolve their operations, choose their partners (both direct partners and those downstream, across networks), and realize efficiencies through automation even while extending operations across the EU. Further, such an approach will enable integration and interoperation with many other financial and information services, including those for consumers and small- and medium-sized business.

These requirements are also key to providing a suitable basis for innovation in new services such as those related to *choice of entry point*, above, and *cost, transparency, and transaction reporting*, below, and in areas such as assurance, security, policy, and liability.

5.5 Central Bank and Regulatory Control

Several countries (e.g., US with the Sarbanes-Oxley Act, UK, France, The Netherlands) and EU regulators (revised EU 8th directive) have recently launched new regulations on corporate governance. Most of the regulations include a requirement for corporate senior management to explicitly state that they have implemented and effectively operated a risk management framework. Typically, these frameworks are based on best practice standards such as Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Effective operation of a risk management framework means that internal controls have been designed, implemented and maintained to identify potential risks and trigger corrective action where necessary.

The effectiveness of such a framework can be enhanced when processes are highly standardized and supported by appropriate automated procedures. Automation of key controls makes companies less dependent on adhering to manual procedures, which are subject to maintaining sufficient discipline in performing the controls. Another advantage of a high degree of automation is that data is gathered on life cycle events that can be used by management to monitor relevant developments. Management can view the exceptions noted in the context of the total of all business events rather than investigating individual exceptions.

TWIST encourages companies to improve their control by implementing standardized, highly automated processes. As far as possible, the standards should not just focus on the normal business operations, but also extend to routine types of exceptions. Examples are the payment status messages that have been developed within the IST Payment Kernel and TWIST Dispute management messages for electronic invoicing.

5.6 Governance of Payment Services Provision

In order to create a more level playing field for the future provision of payment services, consideration should be given to the governance and management of the payment schemes and the infrastructures which support those schemes. As mentioned, for an open architecture model with interoperability, extensibility and robust composability, the development of architectures needs to be managed and controlled within standards development organisations that are fully independent from operational service providers or technical infrastructures.

In particular, the market is moving towards the separation of the payment schemes and the infrastructure providers. For example, in the UK, the former BACS entity has been split into BACS Payment Schemes Limited (BPSL), which is a not-for-profit, membership-based industry body and Voca, an infrastructure company which provides payment services to the market. By contrast, SWIFT, the de-facto payment infrastructure for much of today's cross-border payment traffic in the EU, continues to combine the functions of setting payment industry standards with providing infrastructure and technology to deliver payment services.

Many of the infrastructure providers within the SEPA remain owned and controlled by the banks, and in some quarters, concern has been voiced that these are therefore driven by the agendas of the banking community, rather than in the wider public interest or focused on pure economic motives of the infrastructure providers themselves.
These concerns could perhaps be addressed if ownership criteria were widened, and if the boards of ACHs and other cooperatives were to appoint independent directors tasked with running the organisations based on the pure economic interests of their organisations, within the applicable regulatory framework.

As a result, the combination of choice of entry point, standardised access with predictable service provision, portability of accounts with increased customer mobility and the separation of payment schemes from infrastructure providers might drive those infrastructure providers to compete within a more transparent and open environment based on their own, economically driven parameters.

5.7 Identity and Attribute Management

Management of identities and the related attributes is a key enabler to realizing corporate requirements, both for operational security and for new and innovative service offerings. Current payment mechanisms generally adequately address needs related to controlling access to networks, to data, and to processes. To achieve our overall goals, however, including end-to-end automation across the whole supply chain, and flexibility in clearing and settlement, our interests extend to capabilities concerning secure, compliant, and privacy-protected interoperation across trust domains.

Currently corporates, their customers, and their banking partners, use a wide range of identifiers, from different sources, which are often not generally inter-operable. Identity information, such as certificates are may not be trusted outside the closed community within which they are issued. Identity management under the new regime should retain existing capabilities, while allowing different trust domains to utilize a variety of identifiers—identifiers suitable for different trust, security, and privacy requirements, and identifiers introduced to fit new purposes. However, these different schemes also need to be inter-operable.

Through discovery of and subsequent operation with the appropriate authorities these new identifiers will offer a means to specify requirements for, and verification of, credentials, including the concerns of validity, timeliness and strength. The results of these operations may inform authentication and authorization decisions, and may provide a gateway to discovery and inspection of further attributes (such as concerning role, characteristics, and other identity-enabled services).

In this new world, we believe that it is a key requirement that the *identity owner*, and not the service providers, who can realize ultimate control over their own data within the trust network. This conclusion is driven by the increasingly pressing need for capabilities to select new partners, to alter payment flows, designate and update authorizers, to designate or move accounts, and to inform customers of pricing and terms and offer them actionable choice, possibly in real time. Identity services are crucial to each of these.

For corporates, mandates such as “Know Your Customer” require an ability to request appropriate information as needed, while avoiding the burden and privacy risks of replicating customer information throughout the networks. Features of identity management as mentioned above, and those such as opaque identifiers and identity-related key management provide further protection against unnecessary exposure of customer and transaction information to intermediaries while preserving mechanisms in pursuit of anti-fraud, anti-money laundering, and national and international security interests. These same features enable parties, such as a corporate and a bank, to engage in and complete a transaction, with full trust and assurance, without necessitating the full account opening process generally required today.

These concerns apply to payments made in all forms. Whereas corporates will likely use their pre-existing PKI infrastructures (including smart cards and tokens) to underpin this new identity infrastructure, consumers and small- and medium-sized enterprises may utilize a broad range of means and service providers for establishing and managing identity and the related attributes and services. Whether for corporate payments or consumer payments via mobile phones, the identity operations must be the same.

5.8 Cost, Transparency and Transaction Reporting

The opportunity for significantly reduced costs and improved transparency of cost versus service received, provide the buy-side with clear incentives to invest in process change.

Current payment processes across Europe often do not have a transparent direct pricing model, where corporates can relate individual charges directly to the service performed.

In most cases, service charges do not reflect the direct costs associated with the service. Instead, indirect charging mechanisms are applied such as generating float based on the time lag between processing the debit and the credit transaction.

We believe that there should be a drive to create innovative standardized processes, where it is clear which services are performed and a fee is charged that clearly reflects the nature of the service and associated cost. This can vary from processing charges to risk transfer charges.

When consolidating the processing of payments in the Euro-zone, economies of scale can be realised that could be reflected in the cost per transaction and consequently the processing fee.

Banks can provide more transparent services in terms of risk transfer with credit checks (balance verification), guaranteed delivery (irrevocable payments, where the bank guarantees processing after initial verification) and services that enable reversing the transaction within the legal restrictions as determined by the Commission's New Legal Framework in combination with domestic laws of countries involved.

On top of the basic functionality, banks may decide to offer more sophisticated service levels (e.g. in relation to verifying mandates for direct debits) for which they can request a fee. As it develops, the market will show whether there is an appetite for such services.

In balance and transaction reporting, corporates would like to make the processes to be as transparent as possible. Transparency enables adequate and timely reactions to events occurring. For example, part of working capital management is to manage the daily cash flows of the company. Timely information on realized and expected future cash flows (with an indication of their relative certainty) will enable companies to manage their cash pro-actively and move funds between accounts. For timely business decisions, (expected) balance reporting is most relevant. In order to ensure that the cash flow forecasts in terms of balance reporting are sufficiently reliable, transparent transaction reporting is required where actual cash flows can be reconciled to the expected cash flows. Furthermore, transaction reporting with sufficient level of detail and unique identifiers is required to ensure that operational processes such as accounts receivable and accounts payable reconciliation can be automated as much as possible.

5.9 Implementation and Migration

Transition to any new form of payments model is going to be costly and time consuming. This is mitigated by the fact that technology has moved on and offers new opportunities to isolate change from core systems and deliver new services cost effectively. So great are these costs and difficulties, however, that such technology must be chosen so as to offer corporates direct leverage in areas far beyond payments, extending into other core operations and well into direct services to customers and partners. It should also enable banks and other service providers to generate new revenues through the introduction of new services which have value to their customers.

The key areas where implementation work is required are in the provision of directory services and other universally available services for the delivery of identity and attribute information and the assurance of trust and management of risk, to a degree appropriate for the specific transaction. It is this area which will require the greatest thought and development before the full benefits of the new open architecture can be realised.

We therefore expect that the transition will happen over a period of time, in a number of cycles dictated by the market both from a corporate and Financial Institution viewpoint. Corporates will not only need to show demand for the new more open services but actually need to enhance their capabilities to take advantage of them. At the same time they will need to engage with banks in a way that builds benefits rather than simply increasing price-based competition. So corporates will need to be proactive in developing new propositions that offer benefits to Financial Institutions and drive positive change.

At the same time, banks are already looking at how they can enhance the strategic architectures they are implementing for payments, to be more component or service based, as well as enhancing flexibility and giving them the ability to move to this new model without major change to their core systems. Key to their desire for change will again be the ability to recognise and deliver benefit to their stakeholders rather than just incurring further cost.

5.10 Operational and Non-Functional

Payments underpin the whole fabric of doing business and as such the economies of all countries. Therefore, it is important to ensure the security, reliability and resilience of the underlying systems so that there is no interruption to their operation or systemic risk to the parties using them.

- Resilience to machine or software failure should be built in and monitored closely to ensure no interruption of service
- These services must be highly reliable, ensuring continuity of service and having disaster recovery plans in place and regularly tested to allow for any foreseeable contingency.
- The operational processes underpinning the services must have clear and regularly tested business continuity plans and assets in place to enable these should the need arise.
- Security at a system and operational level is a clear requirement and should be delivered and tested at all points in the chain to internationally recognised standards to minimise the risks to all the parties.
- Central banks and other key market infrastructure providers will have the responsibility to monitor operational risk and in themselves have the Business Continuity and Disaster Recovery capabilities in place to ensure uninterrupted delivery of settlement and support services.

It is also important to ensure the financial viability and soundness of the companies and financial institutions delivering payment services as their business collapse could create disastrous disruption to the delivery of payments in particular at a local or regional level.

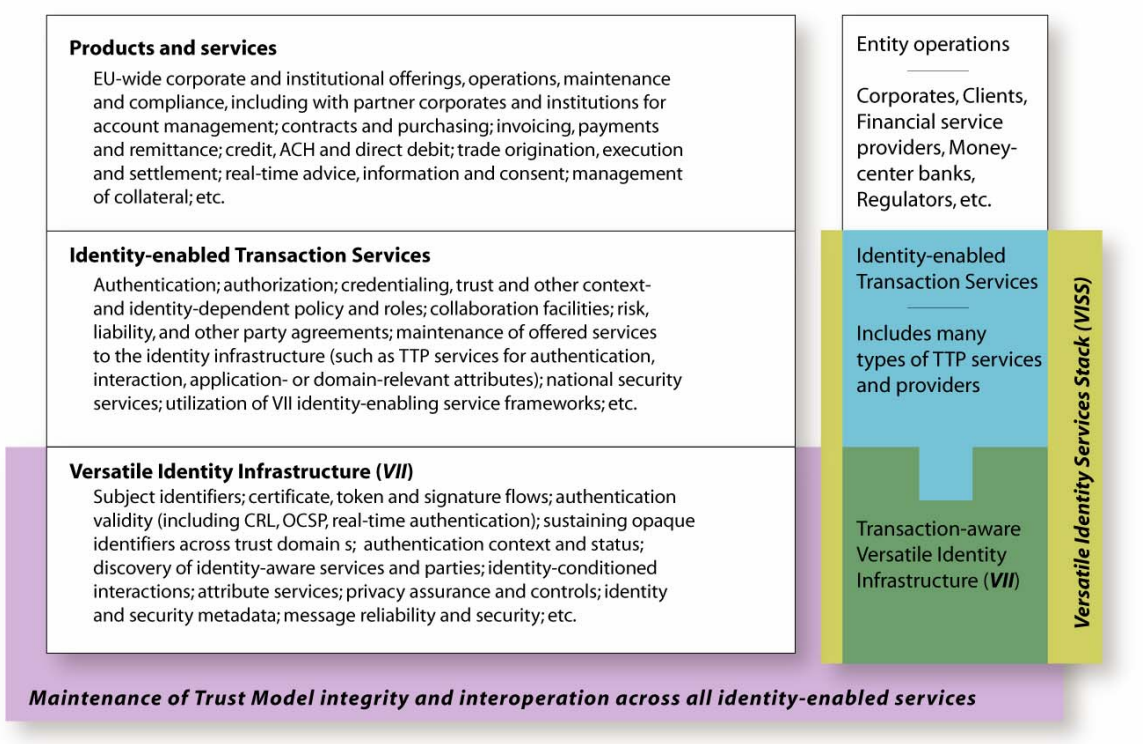
- Whilst licensing authorities should carry out financial checks, corporates themselves should be aware of the financial stability of the providers they are using and the risks they are undertaking much as they do when making investments with a wide range of financial institutions.
- The quality and enforceability of agreements between providers and with corporates must be strong as a breakdown of these resulting in multiple claims and counter claims could cause a breakdown in the whole fabric of payment services.
- The legal enforceability of individual and bulk files of payment instructions is also paramount, as the ability to repudiate these could force a supplier into financial failure.
- As with the delivery of all commercial services providers should be able to charge appropriately and be free from anti-competitive practices or constructs that corporates, large market participants or governments may seek to put in place. Without fair practice the best services may not survive and flourish to the benefit of all.

6 A Potential Systems Architecture

6.1 Summary Architecture

A potential high level architecture is depicted in the diagram below. Much of this already exists in a number of forms, but in many cases is not externalised to allow for use in an industry wide open architecture.

We comment on some of the key enablers for such open architecture in the following sections.



6.2 Trust Model

There are a number of models in the market place. Of these, only some models are capable of scaling across multiple trust domains and across a gradient of trust assurances and risk assignments. Such models implement the concept of interoperable Trusted Third Parties (TTP).

The concept of interoperable TTPs provides for the verification of credentials and other attributes to be carried out in a distributed community, and for the offering of assurances to relying parties. Relying parties, such as corporates, indicate their acceptable TTP's, according to contextually-dependent policies for the levels of authentication appropriate for the desired trust assurance and risk assignment. In some cases this authentication is conveyed in a further credential (for example, a certificate); in other cases this authentication is conveyed in a response to requests from qualified relying parties. In all cases the TTP provides the ability for relying parties to inquire about and verify the current validity of the authentication status. Such systems have wide use among corporates, including mutual, bi-lateral, reliance by one corporate on their partner corporates, to act as a TTP.

Legacy deployments of digital certificates within a public-key infrastructure can perform this function within a single trust domain; modern PKI architectures can operate across external trust domains, especially those architectures having integrated methods for discovering local and external TTP's. Corporates have significant investments in such systems. As the legacy architectures are upgraded to modern architectures such systems will, must, and are capable of, playing a key foundational role in the trust model. To this must be added the ability to specify and rely on the verification of a variety of credentials, for a variety of authentication forms, and request and validation methods. Each such variety is suitable for a variety of secure, trusted, and identity-enabled services.

The system then revolves around the degree to which the party relying on the authentication (evident in a certificate or another assertion from an appropriate and competent TTP) trusts the depth, scope, and timeliness of the vetting and proofing on identity attributes and credentials (including at-the-moment real-time re-verification), and the security and responsiveness of the infrastructure carrying the services. This trust is weighed against the risks and value associated with the transaction, be it financial-, informational-, entertainment-, or security-related.

Underlying this trust model there has to be a set of legal agreements, policies and practices that ensure each of the parties understands and stands behind the obligations shouldered for the given transaction. In many cases because of a bank's unique level of identification and knowledge of a customer they are well placed to be a TTP and offer this type of service for the purposes of underpinning financial transactions.

However, this type of service can also be delivered by other major organisations or government bodies, and even independent corporates and service providers, who have the financial and reputational standing, and who have knowledge of the individual's identity attributes and credentials appropriate for the desired trust and risk. For example, a wireless infrastructure provider may be the best TTP to provide real-time authentication of the geolocation-related credentials and attributes for a transaction. In general, the individual (whether a real or legal person), whose identity is at question controls which TTP is brought into a transaction or service exchange; relying parties may proceed on that basis or suggest (or require) alternates.

One important characteristic of the trust system described above is that it does not require the issuance of a standardised, unique customer identifier (such as an International Bank Account Number IBAN) as the basis for the identity infrastructure. Identifiers of many types are possible; some identifiers may be opaque to all but the principal being identified and the designated TTP.

This is an appropriately versatile system, advancing capabilities important to corporates and consumers alike, such as customer mobility and account portability. Although attractive for the simplicity of explanation, a single unique identifier places significant burdens for administration and reduces the richness of identity on which marketplaces thrive and evolve. What is most required for this capability is what is required in any case: technical languages and systems for describing and exchanging levels of policy, trust, risk, and authority; for enabling real and legal individuals to designate qualified TTPs; for locating the designated TTPs; for TTPs to interoperate, bridge, proxy and delegate such requests; and for requesting or verifying or escalating various acts of authentication and re-authentication.

What have developed in the global marketplace over the last several years are systems that provide a way to bring these advanced identity capabilities into interoperation with modern architectures for certificate systems. These systems allow more flexible and extensive specification of the desired authentication and assurances, including through reliance on certificates.

For example, such systems allow a transaction party, perhaps a mobile carrier, to authorize a particular user identity to proceed with a transaction up to a certain value on a particular account. Then for authorizing amounts beyond that threshold they require and request new authentication assurances based on different identity credentials and attributes, possibly from a different TTP (one with procedures appropriate to the context, a bank for example), and probably for different levels of trust assurance and risk assignment, and at greater expense. In short, each type or level of authorization may require different types or levels of authentication, which are likely to be associated with different TTPs, for different guarantees of trust assurance and risk assignment

Further development of this identity infrastructure will be needed, to fully deliver against this requirement. , , This development will need to extend and enhance capabilities similar to those found in federated identity management services such as the Security Assertions Markup Language (SAML) and the Liberty Alliance.

6.3 Liability Management

Once an identity has been verified and the user has been shown to have the credentials, authentication, and attributes necessary to carry out the transaction they are requesting, (e.g. please pay an amount from my account with X Bank to an account with Y Bank), the relying party will need to know that the paying and receiving banks can and will support the exchange of value. This will create a liability between those two institutions and this in turn needs to be managed and underpinned by rules and fiscal management through central banks so as to limit the risk of individual bank or systemic failure.

Current models are in place to allow this to happen in-country and these are being enhanced to enabling cross border liability management. However, if local ACHs and equivalents start to take payment files from many corporates around Europe who do not necessarily bank with one of the institutions they usually deal with, then a further extension of the liability model will be needed. The processing agent will therefore need to have the ability to check the financial standing and obtain authorisation for payments in real time to enable it to settle them. Architectural models for this already exist in the card settlement arena and these should be capable of being replicated in the SEPA environment.

6.4 Enriched Message Standards

While payment initiation messages are well understood and defined by network operators such as SWIFT and ACHs, many of these message types are based on legacy standards. These messages were designed many years ago to optimise data carriage to the then available bandwidth and inevitably restricted the size and content of messages. As more modern networks have become predominant, for example, SWIFTNet and Broadband internet, it is no longer appropriate to handle data in this way. The use of XML-based messages, such as the IST Payment Kernel developed by IFX, OAGi, SWIFT and TWIST, provides a standard that addresses the needs for corporate customers and banks alike.

The most common impediment to data being carried through the payment system (bank, ACH, RTGS and SWIFT) is erroneous or incomplete information being transferred into the payment reference field, and/or truncation of this information. In either case, this lack of payment reference data, limits the ability of a recipient to link the message back to an underlying invoice.. Furthermore the capacity of payment messages to carry information related to the payment purpose or beneficiary is limited. This is particularly the case, for example, where a single payment covers multiple invoices, or part of an invoice. It is imperative that such reference information as is sent with the payment instruction, or file, and is carried through the payment chain to the beneficiary bank statement. With this in place, the reconciliation of payments to remittance and invoice information could be automated, generating huge savings in productivity for the corporates.

This requirement is not without its challenges. As observed above, most payment systems are restricted in both the range and content of information that can be covered: in the case of ACHs this reference field often no more than 18 characters in length. It is clearly not practicable in such circumstances to carry a large amount of data relating to non-financial information in such a message. Instead, many companies rely on remittance advices to supplement the underlying information that can be carried through bank networks, over the internet or through post or fax. Linking the remittance information to the underlying payment and statement by means of a unique identifier carried on the payment message, the remittance advice and the bank statement will provide sufficient information to enable a reconcile an invoice to a bank statement.

The process of trying to link payments back to underlying data currently is very problematic. SEPA provides an ideal opportunity to change the formats to allow enough data to tie the payment to one or more invoices as well as informing beneficiaries about the reasons for paying partial amounts or making deductions to the invoiced amount. Such information is often generic, meaning that the same data structures can generally be used across industries.

Once the collection of relevant information has been achieved, a major enabler of Straight Through Processing (STP) is the ability to create an automated process that identifies exceptions and

enables the management of those exceptions. This presupposes the ability to import information into an ERP, cash management or other reconciliation or credit management application without re-keying or significant manual intervention. This task can be simplified by identifying the main parameters of the data to be captured and then enable it to be imported according to a common API. It is recommended that as part of the work of SEPA thought is given to ways in which APIs can be made available on an open basis so as to allow simple integration of data. This integration is a prerequisite to achieving genuine, end-to-end, STP.

As many corporates, banks and other institutions move towards Service Oriented Architectures, they will be able to plug in and utilise pre-prepared message adapters or gateways that can format messages both in terms of structure and network protocol. Configurable systems which then orchestrate the processes to make use of these, will be either available or built on flexible IT infrastructures to allow for the addition of a more diverse range of formats whilst insulating current back office systems from wholesale changes.

6.5 Operational Services

To enable corporates and banks to make decisions on which settlement mechanism to use for certain payments, they need to know both the capabilities and and the price that will be charged for each potential provider. They also need potentially to pay the fee at the time that instructions are placed.

Again this generates a requirement for regularly updated directory services which are available to all the participants for comparison and costing purposes. As well as holding pricing information, the directory mustalso define the service level offered, and the cost of repairs or of handling incomplete instructions.

The trust model and summary architecture provide a method for these characteristics to be declared, published and updated, to be available for query or notification, and to be discovered, via the identity infrastructure. In this way corporates could publish real-time schedules of preferences, and banks could publish real-time schedules of capabilities, with service providers offering identity-enabled transaction services to arbitrate between the two.

Externalising this type of information has been seen for some time in the Electronic Data Interchange (EDI) arena and transferred into many vertical trading hubs that have developed on the web to enhance the procurement process for corporates.

7 Impact on the European Payments Market

By enabling corporates to use different providers for individual or blocks of payments, the market will be opened up to much stronger competition at a local, regional and potentially global level.

Service providers will need to compete not just on price but a range of other attributes that will drive competition in the market place;

- Range of services – the ability to offer processing for a wide range of payments or specialise in specific types, geographies or values.
- Service Levels – the quality, reliability, STP capability and timeliness of service can be a delineator in choosing a provider.
- Added Value Services –
    - The ability to deal with remittance and other data connected to the payment.
    - Enhanced payment tracking and confirmation of delivery.
    - Reconciliation services extending those currently available through lockbox products.
    - Full outsourcing of Account Receivables and/or Payables.
    - Enhanced Balance and Transaction Reporting
    - Innovative working capital financing products.

Enhanced competition and greater flexibility of delivery will also likely drive consolidation of services into a smaller number of payment providers further enhancing competition. Potentially, in the medium to long term, smaller providers who operate in niche or specific geographic markets could be driven out of business.

As these changes take hold corporates will also have to change their systems to be able to take advantage of these services and to move away from services that become obsolete or unprofitable to operate in the future.

8 Conclusion - Key Enablers for the True SEPA Vision

A number of internally consistent services needs to be available, to enable the suggested architecture to be implemented.

In some cases industry and governmental regulation will need to underpin these to ensure they are implemented consistently and securely, and that they do not impinge on any current regulation particularly relating to identity management.

1. As mentioned earlier, from the perspective of European treasury associations, the New Legal Framework's coverage is good and it successfully manages to identify the sorts of topics that need to be included in national legislations so as to facilitate the development of the actual payments systems and processes for SEPA by the commercial sector.

2. Trust models need to be built and underpinned by legal agreements that can be enforced across all borders where transaction flows will occur under that scheme. The parties who offer these services will need to work with users and system vendors to agree the technology standards and their implementation within their solutions so that true interoperability can be achieved.

3. As well as the need for technological standards and inter company agreements there will be a requirement for harmonisation of the legal standing of Trusted Third Parties, digital signatures and privacy legislation. Some of this is already in place, but further work will be required to ensure these are aligned and also fully understood by the industry. This is important to ensure that they are implemented without the possibility of creating a loophole to enable the repudiation of payments in a court. Therefore there is a clear role for the Commission in supporting the banks to deliver against their obligations to implement a SEPA.

4. Payment processors, in particular banks and ACHs, will need to look at how they can externalise certain services whilst building on the trust model to ensure the security and privacy of the data exchanged.

5. As these services are externalised, directory schemas and message standards will need to be agreed and published to enable all of the parties to make use of the information available in particular that relating to Service Level Agreements SLAs and pricing for services. These need to be managed by a neutral, trusted party.

6. As a whole the banking community, including the central banks, will need to agree on a liability model that will support and encourage an open, competitive market whilst maintaining its financial stability.

7. Corporates need to become far more active not just driving changes that will reduce the cost of payments but also demonstrating how they will support a more open and diverse market. They must show that as banks' traditional income streams in payments are eroded, there are viable alternative product lines which add benefit to the corporates' businesses, and are therefore revenue generating. Banks will also be key to building these propositions, but as the past has shown us they need the support and guidance of users to ensure they are a success. Without this support and investment of time, banks will simply deliver their vision of SEPA at the lowest cost and greatest benefit to themselves.

8. Technology suppliers see this as a large opportunity, due to the scale of the changes that are to be implemented. However, they need to be encouraged to develop solutions which provide SEPA support in a flexible and open way to the benefit of the overall market. Adherence to standards, use of open source schemas and messaging plus the building of solutions in component form for use on a services basis will all be critical not just to the initial implementation and to an accelerated adoption of SEPA, but also to the future extension of these services.

It is not the function of this paper to define a timescale and true roadmap to implement this vision. However there is an obvious need for greater communication and support for change from all parties, and recognition that this is not a just a bank issue, but an issue for all parties who make, process, settle receive, and reconcile payments.

Appendix 1 – The Regulatory Context for this White Paper

1. **New Legal Framework** NLF, Consultation COM(2003)718, and involving 95/46/EC exceptions related to Article 13(d), Regulation (EC) 1/2003, Directive 2002/47/EC, responses in MARKT/4005/2002): An identity infrastructure makes its greatest contribution in removing the impediments and burdens that led to abridgements of goals. Reporting is more richly facilitated, interoperability in signature recognition is more broadly possibly, collateral arrangements are freed of many procedural and administrative burdens, and number portability and customer mobility is made possible while protecting and enhancing timely and 'effective advice' on costs and options.
2. **Markets in Financial Instruments** MiFID, EU Directive 2004/39/EC (ISD2), and involving the recent (19Oct05) MiFID JWG: An identity infrastructure contributes greatly to satisfying the requirements to improve party identification, for sharing an variety of attributes, and for discerning roles. Additionally, the challenges of informing clients throughout the pre-trade to post-trade cycle is transitioned from a problematic burden to customizable opportunities. The infrastructure can also enable a much richer conception with respect to best execution—that is the broadening of the envelope concerning this goal from primarily transaction-time performance to the larger pre- and post-transaction information sphere.
3. **Industrial Policy**, COM(2005)474 and SEC(2005)1215 et seq: Achieving innovation and intellectual property development significantly depends on cooperation within and among the enterprises, and with external sources of innovation and collaborations. Acceleration of partnering and other enterprise reorganization and cooperation are also critical. This concerns all industries, high tech as well as the traditionally staid. Each of these are areas for impact by an identity infrastructure.
4. **Payer information accompanying funds transfer**, Proposal 2005/0138: An identity infrastructure removes many of the impediments which are assumed in current proposals. Identifiers are given broader roles, which, among other results, enables privacy-protecting interoperation with intermediates and other parties, including those external to the Community, while avoiding the ill-considered forward-transport of information. Other services are improved, while also providing better policing and increasing security against abuse.
5. **Entry and operation in credit business**, Proposal COM(2004)486 (adopted Oct05), esp. in respect to Act 1 and its annex but generally applicable throughout the discipline of regulatory capital: The need for real-time information flows, concerning shareholder identities and the credit conditions of borrowers, places value on privacy-aware identity information, including over a broad collection of attributes. To this we must add the interests of a variety of parties to enter the business, many of whom will wish to collaborate with other parties to provide services (and thus will value a versatile identity infrastructure).
6. **Shareholder information and rights**, Giovannini Barrier 3, regard corporate actions, esp. in respect to investor rights and activities, and involving guidance from CESR and Market Abuse Directive 2003/6/EC: The minimum requirements for notification, and the requirement of guarding against improper disclosure might otherwise constrain the scope of activities in this area. With an identity infrastructure, however, participants gain the ability to directly contact shareholders, to enhance communication of voting or proxy instructions, and to effect direct and timely disclosures.
7. **Cross-Border Payments**, among other, EC Regulation 2560/2001 and the Commission's Consultative contribution of 19Oct05 MARKT/H3 D(2005), esp. regarding continued challenges with identifiers, marking both the need to resolve the problems in the IBAN-plus-BIC scheme beyond just Community banks (2560/2001 targets *retail* as much as bank-to-bank operation): In this area a versatile identity infrastructure could allow essentially arbitrary customer-level identifiers, facilitating resolution to this challenge while also serving in issues of number portability, customer mobility, flexibility and further options in directing payments and settlements, providing access to delayed information.

8. **Data protection**, in various respects, including directives and requirements deriving from the Data Protection Directive (95/46/EC), DPD, the Telecommunications Data Privacy Directive (96/77/EC) the Electronic Communications and Privacy Directive (2002/58/EC), including the perhaps most vexing long-standing challenge of balancing societal security with personal protections (for example the challenge of balance for DPD's Article's 6, 7, and 13): A versatile identity infrastructure provides a way to successively move data out of the reach of inappropriate commercial uses, then a succession of types of data holding for security purposes, while also providing a de-identified yet still integral data source for managing network services. This infrastructure also could provide real-time management of unambiguous consent to sharing of directory information, including self-management and publishing of data limited only by customer choice (such choice being in any of the data dimensions, the requesting context, the automation of such as subscription to updates, customer election of data use solicitations, application of agency to such choice, and more).