

The Critical Role of
Identity Authentication in SEPA
and Cross-Border Payments Initiatives



All You Need is One.
Enabling an eco-friendly digital world.

TABLE OF CONTENTS

Introduction	3
The Importance of Global Standards	3
Legal Issues	4
The Need for Identity Management	4
The Role of the Financial Institution	5
Identity Authentication Crucial to SEPA and Other Cross-Border Initiatives	5
Multiple Usages	6
The IdenTrust Difference	7
Conclusion	8
About IdenTrust	9

INTRODUCTION

Driven by political, regulatory and economic pressures across the European Union (EU), the Single European Payments Area (SEPA) project aims to improve the efficiency of cross-border payments. SEPA will transform the Euro payments landscape from a fragmented nationalized market into a single domestic entity that will enable customers to make Euro payments across Euro zone countries in the same manner they make domestic payments: using a single bank account and set of payment instruments.

SEPA's wide-ranging changes will have a significant impact on issues of trust, reliability and authenticity between counterparties as these issues become exponentially more critical across a much larger ecosystem that spans multiple legal jurisdictions.

To encourage the payments industry to establish pan-European conventions and legal regulations that support SEPA, leading European banks established the European Payments Council (EPC) in 2002. EPC rulebooks form the basis for credit transfer, direct debit schemes and the card framework. Beginning January 2008 until the end of 2010, a new Euro-domestic market that uses a single standard format will replace the existing payments systems.

The Importance of Global Standards

The mass acceptance of the Internet drives the need for global regulatory interoperability. Both companies and consumers communicate with customers, suppliers, partners, and others located beyond their borders. However, lack of global interoperability impedes continued growth by suppressing the opening of markets to the greatest number of firms, increasing the barriers of entry and decreasing competition and innovation.

Moving goods across borders requires identifying and authenticating the buyer and the seller and facilitating financing and payment regardless of where the business is transacted. This process can take 90 days or more, is heavily dependent on paper and typically results in a large number of errors. When combined with language differences, measurement translation (metric vs. universal), and customs import and export regulations, the costs of cross-border selling becomes impossibly high for most small- and medium-sized enterprises.

Although disparate approaches abound, markets themselves tend to consolidate under a global, interoperable, open standard. For example, the world's network of railways--one of the greatest eighteenth century infrastructures--carried fundamentally the same goods of passengers, raw materials, cargo and other livestock. Yet each country and region relied on its own variable-width railroad gauges. These variations occurred for a number of reasons: self-defense so invading neighbors could not use the same rail network; protecting local vested interests and national monopolies; or differences in terrain and local engineering practices.

As a result, moving goods across borders was more complicated, cumbersome, slow and expensive than moving goods domestically.

Today, railways across Europe and around the world use a standard gauge of 1,435 millimeters. This standardization has significantly improved railway transportation. The telecommunications industry is undergoing a similar transformation from country-specific phone jacks and phone systems to standardized phone and Ethernet connections to provide electronic connectivity to people around the world.

Legal Issues

Liability and legal recourse are also inconsistent when doing business across borders. Every country has its own regulatory and legal framework which requires companies doing business in multiple countries to navigate multiple legal environments.

Incorporating electronic rather than paper-based documents provides much needed legal consistency. Andrew J. Pincus, former general counsel to the U.S. Department of Commerce writes, “A viable framework for electronic commerce requires the elimination of paper-based barriers such as “writings” and “originals” and the introduction of electronic means to enter into legally binding contracts.”

Even with electronic documents some legal obstacles remain. In Economic Perspectives, a publication from the U.S. Department of State, Dr. Carlos Moreno, legal officer with UNCTAD (United Nations Conference on Trade and Development) writes, “The extent to which national and international law accepts that an electronic message can perform the same function as a paper document differs considerably. Most of the international conventions and national laws that were adopted more than twenty years ago did not, as a general rule; anticipate the possible use of electronic means of communication. This is largely because such means of communication did not exist when these international conventions and national laws were drafted and the necessary modifications to them have yet to be made.

“Furthermore, many national laws also introduce uncertainty regarding the legal validity of electronic-based transactions or are inconsistent in their treatment of new technologies. Also, few courts have had the opportunity to rule on the validity of electronic documents, messages or signatures.”

SEPA is proactively developing the legal framework to support cross-border payments and provides an example of standardization to the rest of the world.

The Need for Identity Management

Identity management is a widely-used phrase that has different meanings. In the context of SEPA, identity management is closely aligned to risk management: having a degree of certainty that the counterparty to a transaction is who they purport to be based on support by one or more trusted intermediaries to whom or from whom a payment is being made across the SEPA geographies. To be truly “trustworthy,” this risk management framework must allow parties to interact in an environment of privacy, authentication, message integrity, and non-repudiation by provisioning credentials which enable authentication, encryption and digital signing.

One of the most difficult identity challenges is making certain that people really are who they say they are. Many identity solutions today are called “self-signed” or “self-asserting” because the identities are not verified by an independent third-party. Financial institutions meet this challenge by requiring that customers provide multiple forms of identification before opening any type of banking, insurance or capital markets-related account or transacting payments. This federally-mandated process, called Know Your Customer (KYC), applies to both individuals and corporations and requires the same stringent controls and level of trust for digitally-issued identities.

A globally consistent approach to digital identity due diligence, similar to payments due diligence, can provide identity transparency. Disjointed, non-interoperable identities give rise to industry inefficiencies, additional costs and greater risk. A patchwork of different identity schemes across national or geographic borders or industries or products is as

inherently cumbersome as different railroad gauges. Although bilateral agreements have been made between organizations within small communities, they are not scalable on a pan-European or global basis. A rules-based scheme approach, wherein one contract provides watertight relationships and liabilities for all members, is needed.

Financial institutions—typically banks—used to be able to control networks and messaging system entry and exit points. As networks expand and new ones are created, end-users demand direct access, evidenced by the need to provide direct corporate access to SWIFTNet, BACSTEL-IP and now some of the SEPA platforms. Financial institutions are now required to individually identify who actually initiates, signs for and executes a payment--and when--rather than just identifying the corporation the individual user works for.

Lastly, similar end-user pressures related to cost and processing time are causing the convergence of the physical and the financial supply chain. As information flowing between two parties becomes increasingly network independent, the information will flow over whichever route is most ubiquitous, safe and economical.

The Role of the Financial Institution

Financial institutions are best positioned to provide a risk management framework for SEPA and other applications that rely upon electronic and counterparty-not-present credentials. While banks often provide this service today, alternative entities such as governments, other types of financial institutions, or even the end-users themselves can also provide this service.

However, these solution providers are problematic:

- Although governments are massive users of electronic networks and keepers of detailed electronic information (such as tax returns) and have a strictly-defined liability framework, they are not well-suited to managing commercial risks between citizens, businesses and third-parties.
- It's impractical for corporations or citizens to assert their own identities in making or receiving a payment and to manage non-repudiation and dispute resolution for multiple applications across multiple jurisdictions. Like governments, corporations and citizens do not view themselves as managers of the operational risks associated with intermediation between parties.

The natural providers of this critical service, and the organizations whose structures are appropriate for this task, are the world's financial institutions, especially those who see a future for themselves in transaction management.

Identity Authentication Crucial to SEPA and Other Cross-Border Initiatives

SEPA is focused on three areas: credit transfers, direct debits, and the cards framework (although the latter needs clarification). Of these three, many experts believe that the introduction of SEPA Direct Debits (SDD), formerly known as the Pan-European Direct Debiting scheme (PEDD), will be the catalyst for widespread adoption of a cohesive, interoperable, underlying identity authentication framework and a clear liability management structure.

For example, an Irish citizen with a house in Spain needs a Spanish bank account in order for the local utility company to apply a direct debit for gas, water and electricity charges. The Spanish bank will almost certainly have a relationship with the utility company or, at the very least, will recognize the direct debit as a routine transaction. With SDD, the Irish citizen will be able to use his local Dublin-based bank account for the direct debit even though it is highly unlikely that the Dublin-based bank has a relationship with the Spanish utility company. The ability to prove the identity of both the individual and the organization enables the direct debit to occur.

It follows that:

- a) a credential issued by the Spanish bank to the utility company needs to be interoperable with and able to be relied upon and trusted by the Irish bank and its customer, and,
- b) this credential must be authenticated/validated online and in real time.

Extend this example across different geographies, different customer sectors and different products and services and you can quickly understand that multiple bilateral agreements between disparate identity providers are simply not feasible. There must be a scheme--a set of rules which are stronger than codes of conduct, obligations, responsibilities and liabilities--for each of the four parties described in this example. This scheme must scale across Europe and the rest of the world.

It will be crucial for SEPA service providers to manage the identities of the corporate organizations performing the direct debit creation and, more importantly, direct debit collection. Service providers will need a comprehensive audit trail that identifies the individual to improve control and minimize risk.

Multiple Usages

Although SEPA is an important step in the evolution of the payments industry, additional issues need to be addressed. A financial transaction between two parties is invariably preceded by a series of interactions which culminate in the movement of money. During each of these interactions, the need to remain assured that the counterparty is who they say they are becomes as important as the payment itself. Having a separate electronic identity credential for each piece of a transaction is of no value to the end-user; instead, using the same underlying credential is essential. An identity does not change during a transaction, especially when its original issuance is based upon strong KYC practices and where a third-party, such as a bank, can vouch for the identity of its customer.

The same identity used by a corporate to sign SEPA payment transactions with their bank should be used with other transactions where a bank-backed identity credential would add value, such as SWIFTNet, the domestic ACH, the bank's e-banking platform and signing electronic forms through e-invoicing.

The IdenTrust Difference

IdenTrust, similar to SWIFT, Visa and MasterCard, was developed by a consortium of financial institutions from around the world to deliver trusted electronic commerce. Working together, these institutions agreed on rules for authenticating identities to create an infrastructure all members can rely on regardless of which institution performed the authentication. Today, IdenTrust digital certificates and signatures are accepted in more than 175 countries. This number will continue to grow as more global banks are added to the membership.

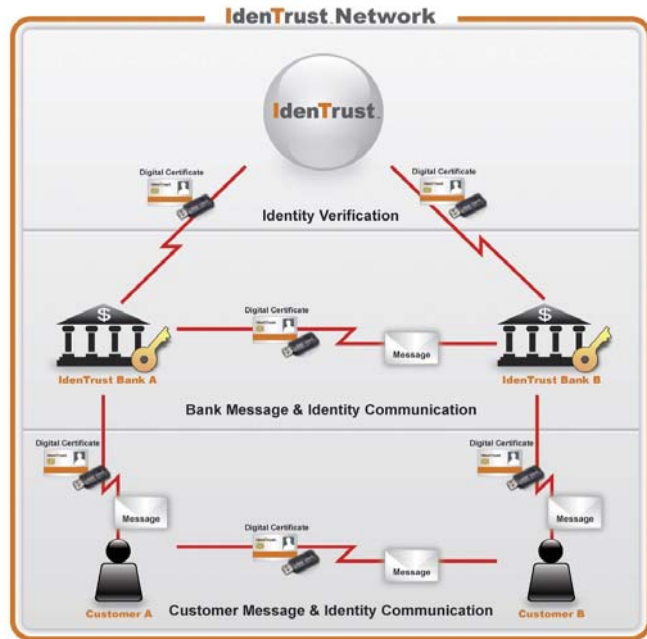
As with customer relationship and risk management, identity management requires consistent vetting, storing and validating. Multiple and unique approaches cause confusion and enable fraudsters to exploit the differences between methods. An enterprise approach to identity management also makes it easier for customers to adopt and adapt to using digital certificates and signatures.

IdenTrust has created identity authentication best practices that govern identity vetting prior to certificate issuance and ensure that identities will be consistently handled across all of the participants in a transaction. Expanding this consortium to include global participants ensures that identities are globally interoperable under uniform private contracts recognized around the world. Unlike most systems which require public law for digital signatures, IdenTrust rules also govern customer agreements and ensure that they are valid, binding and enforceable in countries where the participants do business.

In 1999, IdenTrust adopted PKI because it is the most robust technology for online credentials and identities and ensures that all members are vetted externally before conducting transactions with other IdenTrust community members. Today, most digital identities only provide a two-way interaction between entities such as the user and the bank that issued the online banking credentials. While credentials from VeriSign or RSA provide better protection than a PIN/password combination, this approach is susceptible to man-in-the-middle attacks and other cyber-fraud that works by enabling fraudsters to take over transactions within a computer. Additionally, these solutions are not globally inter-operable.

In the IdenTrust model, banks obtain customer verification information to authenticate participants. Every transaction in the IdenTrust model must pass 18 separate checks before being processed. IdenTrust has two methods to verify a user's identity: following the banks' very rigorous KYC customer verification policies before a credential is issued and a multi-layered, identity verification process when the identities are used for electronic financial transactions and sensitive communications.

Additionally, the IdenTrust model does not violate the privacy of the sender or the receiver. The IdenTrust Rule Set protects against unauthorized access to the transaction information. The transaction data and signed certificate are exchanged between the banks involved in the transaction. The messages related to the transaction data are exchanged between the bank customers on either end of the transaction. IdenTrust only validates the identities used by these customers, not the data associated with the transaction. The transaction data itself is never passed to IdenTrust. It remains with the banks involved. Please see the figure below for an illustration of the data flow and the privacy protection inherent within that flow.



To simplify adoption and ensure trusted identity authentication, IdenTrust conducts a secure operation auditable with the same stringency applied to financial institutions. End-to-end activity tracking required for regulatory reporting in jurisdictions around the world is a key part of the IdenTrust value proposition. Also, the IdenTrust operational environment is easy to integrate with other trust-related products and services (e.g. USB, smart card, roaming certificate, and encrypted USB drive), enabling financial institutions to more rapidly extend their compliance spectrum.

CONCLUSION

Technology continues to change the way we communicate and do business globally. To facilitate this evolution, regulations must be globally interoperable to enable participants to rely upon authentication anywhere in the world.

Creating identity authentication best practices requires a comprehensive approach. Addressing technology or operations provides only a piece of the solution. A legal framework that includes interoperable contracts, agreed-upon policies and procedures for issuing and revoking certificates and liability agreements is required.

SEPA is happening. It will provide significant streamlining opportunities for the corporate user, the government user and the citizen. It will cut costs and lead to faster money transmission speeds and bring the physical and financial supply chains into closer alignment. However, for SEPA to reach its full potential worldwide, it is essential to create a framework to manage the operational risks associated with the issuance and reliance of electronic identity credentials. A patchwork of solutions is not sustainable.

As SEPA consolidates banking relationships, the financial institutions that will gain most are those that implement identity authentication solutions for their customers.

ABOUT IDENTRUST

IdenTrust is the global leader in trusted identity solutions, recognized by global financial institutions, government agencies and departments, and commercial organizations around the world. IdenTrust enables organizations to effectively manage the risks associated with identity authentication; work interoperably with countries around the world; minimize investment in creating their own policies and legal frameworks; and deploy a spectrum of products insuring trust, smarter, faster, and more cost effectively.

The only bank-developed identity authentication system, IdenTrust provides a unique legally and technologically interoperable environment for authenticating and using identities worldwide. The IdenTrust Trust Infrastructure is predicated on a proprietary framework that combines policies, legal framework, trusted operations and technology (PLOT) to create a comprehensive environment for issuing trusted identities. IdenTrust is the only company to provide a solution incorporating all four of these elements. Customer agreements are valid, binding and enforceable in more than 175 countries. IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Competing offerings, in contrast, require participants to navigate a confusing maze of public laws that vary from jurisdiction to jurisdiction. Additionally, the IdenTrust Trust Infrastructure maintains the privacy of each and every transaction processed by reading only digital certificate information, not the message itself.

Additional information can be found at www.IdenTrust.com.

Corporate Headquarters

IdenTrust Inc.
55 Hawthorne Street, Suite 400
San Francisco, CA 94105
USA
Telephone: +1.866.IDENTRUST (+1.866.433.6878)
Fax: +1.415.486.2901
www.IdenTrust.com

European Office

IdenTrust Inc.
288 Bishopsgate
London, EC2M 4QP
United Kingdom
Telephone: +44 (0)203.008.8330
Fax: +44 (0)203.008.8331