Identrus-enabled applications

Detlef Hühnlein

secunet Security Networks AG
Sudetenstraße 16, D-96247 Michelau, Germany
detlef.huehnlein@secunet.com

Abstract

This paper provides a brief overview of the Identrus system - a global trust infrastructure for B2B e-commerce, which is supported by more than forty major international banks – and focuses on related business and application issues. We will discuss possible Identrus business models for participating financial institutions and explain the two major phases of application deployment, reflecting the evolution from 2-party to n-party transactions, by considering existing and potential future Identrus-enabled applications.

1 Introduction

Security concerns, and especially the lack of financial warranty in transactions with unknown business partners, have been among the major obstacles to the wide deployment of electronic commerce. While the deployment of adequate security mechanisms in e-commerce-scenarios tends to become standard, all these problems have not been solved in a satisfying manner. Even the celebrated legal recognition of digital signatures in many countries all over the world does not seem to provide a comprehensive solution. In fact, it is only the second best solution to be able to resolve a dispute arising in an e-commerce transaction, and especially the implied financial consequences, more easily at court. It would be much better if there would be financial guarantees right away, because in the end the assurance of payment / delivery, and not only the assurance of identity, is what counts.

To provide financial warranty and payment guarantees within business transactions has been a typical service provided by financial institutions all over the world. Therefore it is not surprising that banks are keen to provide this service in e-commerce scenarios as well. On the other hand, as the internet makes it easier for parties to communicate directly and hence traditional value-chains are repeatedly broken and re-formed, the banks need to take care that they do not suffer from disintermediation.

In view of these threats and opportunities, eight major international banks - ABN AMRO, Bank of America, Barclays, Chase Manhattan, Citigroup, Deutsche Bank, Bankers Trust (in the meantime acquired by Deutsche Bank) and HypoVereinsbank – joint forces in April 1999 to create Identrus LLC – a for-profit organisation with the mission to provide a global trust infrastructure for B2B e-commerce. Unlike many previous public-key infrastructures (PKIs) however, the Identrus system does not only provide assurance of identity, but – by means of a comprehensive legal framework between Identrus, the participating financial institutions and their commercial customers - also gives rise to enhanced financial services, such as warranties, in global B2B e-commerce transactions.

The scope of these Identrus-enabled applications, in which we are most interested here, ranges from simple 2-party transactions between a bank and its commercial client to complex n-party transactions in which many (potentially unknown) business partners, and their respective banks, are involved.

While there have been numerous papers, which explain how to set up and operate a PKI, the importance of certificate-based applications still seems to be underestimated. In fact, building an infrastructure, as a PKI for example, is inherently a very expensive task. Therefore, in order to achieve a (fast) return on investment, it is most important to design and implement value-adding applications based on this infrastructure. From our experience it seems that there have been many activities to build different "networks of airports" without concisely thinking about the "flight schedules" and for what kind of "flights or on-board shopping-services" the customers are willing to pay for. This paper provides assistance in designing a "flight schedule" for existing and evolving "Identrus-airports", which will compensate investments in the Infrastructure.

This paper is organised as follows: Section 2 provides a brief overview of the Identrus system. Section 3 sketches possible Identrus business models and revenue opportunities for financial institutions. In section 4 we will discuss Identrus-enabled applications. We will clarify the scope and potential of Identrus-enabled applications, discuss a typical application roadmap and some existing applications. In section 5 we will provide the conclusion of this work, which shows that the Identrus infrastructure is more than “yet another PKI” and that there are Identrus-enabled applications, which will lead to a return on investment.

2 The Identrus trust infrastructure

Since spring 1999 the number of banks participating in Identrus has (as of June 2001) grown to 47. As can be seen from the appendix, the list of current Identrus members reads like the “who-is-who” of global financial institutions. Furthermore, Identrus LLC has established strategic partnerships with S.W.I.F.T, which is in turn owned by more than 3,000 banks, and a variety of major international system providers, like Microsoft for example. Considering these facts it seems to be clear that the Identrus system has reached the critical mass and it can be expected that the number of participating banks will keep on growing in the future. As explained in the introduction, the mission of Identrus is to provide a global trust infrastructure for B2B e-commerce transactions. Technically, the Identrus system is a PKI in which Identrus LLC acts as root certification authority and the participating banks act as Level 1, or in the future Level 2, certification authorities, which issue (identity- and utility-) certificates to their commercial customers. To guarantee interoperability, Identrus requires the deployment of widely adopted technical standards, such as X.509 **[X.509]**, OCSP **[RFC2560]**, PKCS#7 **[PKCS7]** or PKCS#10 **[PKCS10]** for example.

The functional architecture in a typical four-corner scenario, which includes a purchasing manager (certificate holder) and a seller (relying party) is shown in Figure 1. Both parties are supplied with a key pair and certificate issued by their respective bank, which acts as Level 1-CA. The private key is stored and applied in a smart card or – for the relying customer, which typically is an automated server – a hardware security module. The certificate status during a transaction is checked online using the plain Online Certificate Status Protocol (OCSP) **[RFC2560]** or a Certificate Status Check (CSC) protocol, which is basically OCSP wrapped

in XML. The sequence of necessary steps and the connection to back-end systems, like the risk management module, is covered by the transaction co-ordinator.

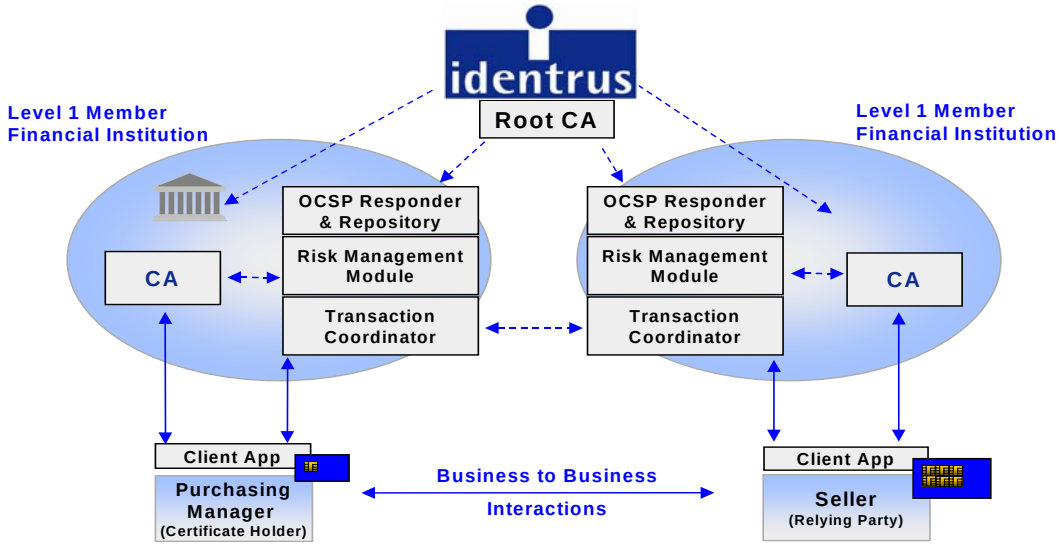

Figure 1: Functional architecture of Identrus system

But Identrus provides much more than a technical infrastructure. There is a comprehensive legal framework covering Identrus LLC, the participating banks, their commercial customers and finally the employees of theses organisations. This means that there are contracts between Identrus LLC and the participating banks and contracts between the financial institutions and their commercial clients (including companies and certificate holders). These contracts regulate rights and obligations of all involved parties as well as dispute resolution procedures. While the Identrus system has global reach, it is in fact a closed user group and hence it is in general[1] not related to public signature laws. Please refer to **[Mill01]** for some more information on legal aspects of the Identrus system.

The presence of this legal framework, in conjunction with the technical infrastructure sketched above, is what makes up the Identrus system, which

provides trust in global B2B e-commerce transactions, including assurance of identity, financial warranty and liability.

It should be stressed, that these commercial issues are not covered by most PKI-initiatives.

3 The business case for Identrus

In this section we will briefly discuss the business case for financial institutions participating in the Identrus system. As the Identrus system aims at a high level of trust and as setting up such a secure infrastructure is expensive, it is more than natural to ask for the business case of supporting Identrus. While the strategic importance of becoming Identrus participant in order to guard and expand current business in view of e-commerce influences is clear to banks, it

[1] The Gatekeeper initiative **[AuOG98]**, where Identrus-certificates from Australian banks are also recognised by local government agencies, seems to be among the first instances where Identrus certificates can be used for B2G transactions, and there is no compelling reason why there should not be more convergence between local signature legislation and the Identrus system.

often demands a more detailed treatment to justify large investments. The question is how financial institutions can earn money by supporting Identrus.

From our experiences the main generic revenue opportunities for financial institutions are as follows:

- Subscription based fees for
  - Subscribing Customers

    The (employer of the) Cardholder will need to pay a (small) amount for the provision of the smart-card, card-reader, client system and certificate.
  - Relying Customers

    The e-commerce system provider will be charged with fees for the Relying Customer's certificates. Note that, as explained below, it is often a good idea to bundle additional (e. g. hosting) services with the subscription of Relying Customers.
- Transaction based fees

  Probably the most important source of revenue is related to transactions, where there are typically applications with a fixed fee per transaction and also applications, e.g. involving financial warranties, which are bound to the value of the transaction.
- Additional services

  What kind of additional services are suited for a concrete financial institution needs to be decided on a case-by-case basis. Potential examples include:
  - Hosting services for Relying Customer applications
  - PKI hosting services for corporate customers and other participants
  - Level 2 services (for smaller associated and foreign financial institutions)
  - Rating and risk management services
  - Validation and warranty services
  - Accounting and archiving services

Note that almost all of the above revenue opportunities are closely related to suitable Identrus-enabled applications. In fact the main motivation for studying Identrus-enabled applications is due to the strong demand for sound business cases for Identrus projects.

A real world business case clearly needs to consider the concrete situation of the financial institution and typically involves most of the above aspects. Please refer to the full version of this paper **[Hühn01]**, the slides of Ian Fullerton's presentation at the Identrus System Deployment Conference 2001 **[Full01]** and the anonymous case study "Identrus at GLOBANK" in **[Secu01]** for more information on the Identrus business case for financial institutions.

4 Identrus-enabled applications

In this section we will focus on Identrus-enabled applications, which are essential to the development of appropriate business cases for Identrus system deployment. The abstract list of revenue opportunities above shows that the typical problem for financial institutions is not the lack, but rather the rich number of business opportunities, which require suitable structuring

and prioritising. This section aims at assisting (prospective) Identrus participants in developing suitable application deployment strategies.

This section is structured as follows. First, in Section 4.1, we will clarify the scope and the potential of Identrus from an application point of view. In section 4.2 we present a typical application roadmap, which may guide financial institutions in formulating business cases which will lead to fast return on investment. Section 4.3 briefly sketches some existing Identrus-enabled applications at the time of writing.

Please refer to the full paper **[Hühn01]** for a more detailed treatment of these aspects and application deployment issues.

4.1 Scope and potential

Before one starts to create an application deployment strategy it turns out to be beneficial to clarify the scope of Identrus-enabled applications. From the point of view of a financial institution, applications may be classified by considering the parties which are involved in a transaction, and the required level of assurance.

While, from a technical point of view, it would be possible to use the Identrus infrastructure for all kinds of applications, there are business aspects, which tend to limit the scope of Identrus-enabled applications. This is due to the fact, that Identrus requires the application of fairly expensive components and mechanisms, such as the deployment of secure hardware tokens and online certificate status mechanisms for example. This implies, that the typical[2] scope of Identrus does not include applications, which – because of the low transaction value – require a very modest level of assurance or never leave the realm of the bank.

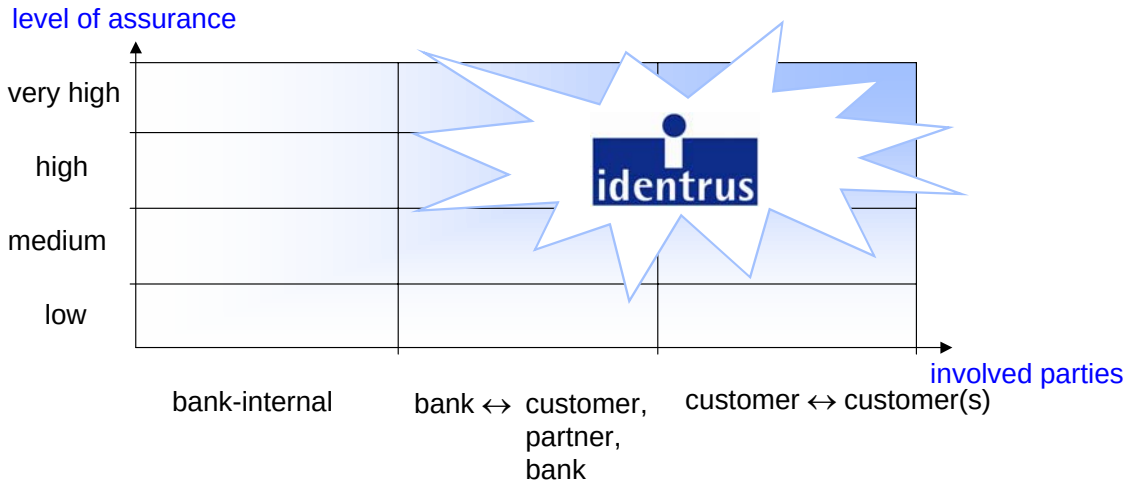

Figure 2: The scope of Identrus-enabled applications

For the remaining scenarios shown in Figure 2, i. e. transactions between the bank and a second party - like its commercial client, a business partner or another bank - or transactions between two (or more) commercial customers, the deployment of Identrus provides significant benefits, as the Identrus trust infrastructure does not only provide assurance of identity and

[2] It should be noted, that in some circumstances it might be beneficial to implement a highly unified trust infrastructure regardless of the required assurance levels.

non-repudiation of origin, but also financial guarantees and regulated liability in transactions between unknown business partners. The latter is very important for n-party transactions between globally operating companies.

Thus, from a conceptual point of view, the Identrus system has the potential to become the de-facto trust infrastructure for global B2B e-commerce transactions. But, there is yet another point to be considered in order to estimate the real world potential of Identrus. It clearly is not sufficient to consider conceptual aspects, but one also needs to consider the market response to this initiative. The nicest concept to implement global trust is useless, if the critical mass of supporting organisations all over the world is never reached. Considering the fact, that the number of participants in this initiative in the last two years grew from seven to more than forty and virtually all major banks in the world (are about to) support Identrus, it seems that this critical mass already has been reached. Due to this broad support of Identrus within the financial service sector, very many e-commerce technology suppliers have been working on Identrus-enabling their products and the number of Identrus-enabled applications will grow even faster in the future. Thus the overall situation may be summarised as follows:

The Identrus trust infrastructure is about to become the de-facto standard for global B2B e-commerce transactions.

4.2 Application roadmap

In this section we will discuss a typical application roadmap, which may assist financial institutions in developing an application deployment strategy for Identrus, which leads to a fast return on investment.

4.2.1 General strategy

As discussed in the previous section, the scope of Identrus-enabled applications ranges from transactions between the participating bank and a second party (customer, partner or bank) to n-party transactions between different customers of independent banks. Considering the current situation in many financial institutions, there are often already established extranet-like (e. g. EDI-based) channels to major customers, partners or other banks. Thus, because these types of transactions are already covered by conventional means, the benefit for introducing Identrus for these applications is fairly[3] limited – the real benefit of Identrus will be visible in transactions between unknown business partners, taking place in open e-markets for example. On the other hand, the support of n-party transactions obviously requires the existence of Identrus-enabled interfaces between a financial institution and its customer, partner or other banks. Therefore it has proven to be a good idea to have two phases of application deployment, when introducing Identrus.

[3] Because these business relationships tend to become much more flexible, the management of all extranet-like interfaces to customers or partners is no trivial task. In view of this situation PKIs, like Identrus, may considerably ease the management of these interfaces.

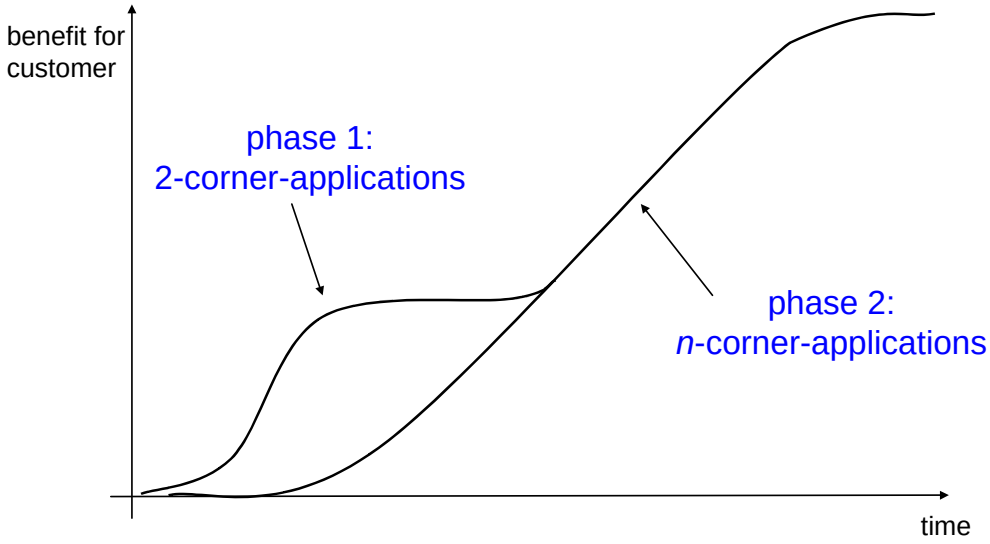

Figure 3: The two phases of Identrus application deployment

As shown in Figure 3 above, the first phase provides Identrus-enabled interfaces to the bank's customers, which can be utilised in simple 2-party transactions, while the real benefit for the customer will become visible in more complex n-party transactions between unknown business partners.

Hence the general application deployment strategy, from the point of view of a financial institution, may be summarised as follows:

> *Start by providing Identrus-enabled interfaces to your customers and partners and successively base new - and combined with additional incentives and value adding services also conventional - applications on this infrastructure. Let your customers know, that this is only the first phase and a much higher benefit will be visible in the second phase, which covers the support of open e-markets and complex n-party transactions.*

4.2.2 Potential 2-corner applications

The 2-corner applications, which could be Identrus-enabled in the first phase, mainly comprise traditional financial services, such as

- account management
- security-trading
- online credits
- commercial insurance sales
- leasing
- bill-presentment, -settlement and -archiving
- initiation of letters of credit
- FX-settlement

for example.

What kind of applications should be chosen for Identrus-enabling depends on the concrete situation of the financial institution.

In particular one needs to consider the general strategy of the financial institution concerning the provision of additional services as well as the existing IT-infrastructures and applications.

In this context it is important to ask what kind of prospective Identrus-enabled 2-corner application(s) will be best suited for bundling with additional services and will allow a smooth migration to the scheduled n-corner applications. Therefore it is important to sketch the entire application roadmap before finally deciding on the applications for the first phase.

4.2.3 Potential n-corner applications

The main philosophy behind the design of Identrus-enabled applications in this phase may be summarised as follows:

- Covering the entire value chain of trading (or project fulfilment)
- Providing additional services in each phase (offered by spin-off-companies and/or strategic partners)

Especially the latter aspect is important to guard against disintermediation or, as multiple financial services are already provided by non-bank organisations, allow reintermediation.

In the following, we will sketch a few possibilities for Identrus-enabled services along the value chain of trading:

- **Finding of trading partner**

  This may be performed with some sort of Identrus-related directory service or search engine. As soon as there is a sufficiently high market penetration by Identrus-enabled applications, it might be an interesting, and from a strategic point of view very important, service to provide a secure search facility for specific goods or services.

- **Offer, bid, selection**

  This step is typically performed in some sort of e-procurement system or e-marketplace. To see that the value of the Identrus system in these steps can go beyond the plain assurance of identity, one should think about possible notary services in online auctions and regulated procurement systems, which may involve trusted time-stamping services for example.

- **Obtaining credit**

  In this step, the buyer needs to obtain credit for a specific deal. This service may be coupled with online-rating and more sophisticated risk-management services. Furthermore this step can be combined with offering financial warranties, e. g. including currency warranties, and the final payment.

- **Logistics/Fulfilment**

  Besides the plain transport of the goods one may think about additional services, like transport insurance or tracking services for example. For the logistic step, Identrus certificates can be used in conjunction with the logistic framework of Bolero **[Bole01]**. In case of service-related projects, Identrus-certificates may be used for securing the project-internal workflow.

- **Payment**

  Handling payments is the classical business area of financial institutions. But, as the discussion above suggests, Identrus is ***not*** limited to payment applications. There has been a project "Eleanor" by a couple of Identrus member banks which standardised the following message types for payment initiation:

  - Payment Orders

    The payment order is revocable by the buyer. The liability rests with the buyer.

  - Payment Obligation

    The payment obligation is only revocable by the buyer and the seller together. The liability rests with the buyer.

  - Certified Payment Obligation

    The payment obligation is only revocable by the buyer and the seller together. The liability rests with the buyer's bank.

  Furthermore it should be noted, that all of the above payment variants may be set up conditional in the sense that they are payable upon fulfilment of pre-agreed conditions. Please refer to **[Slog01]** for more information on the project "Eleanor".

  An alternative[4] to "Eleanor"-payments is S.W.I.F.T's payment product "e-paymentsPlus", which is based on the TrustAct messaging system **[Maes01]**.

- **After sales services**

  Finally the financial institutions will be able to offer after sales services, such as accounting or archiving services.

Besides all these services along the value chain of trading, Identrus certificates may be used to secure *inter-organisational* workflow, which are not directly related to trading of goods.

4.3 Identrus-enabled applications in production

In this section, we will briefly sketch a few of the Identrus-enabled applications in production[5]. Please refer to **[Hühn01]** for more information.

- **Electronic Bill Presentment and Payment (EBPP)**

  There are EBPP systems at Deutsche Bank AG **[DeuB01]**, **[Iden01b]**, and HypoVereinsbank AG **[Land01]**. In these systems the financial institution presents its corporate customers bills electronically and provides means to pay these bills.

-

[4] There are initiatives to harmonise S.W.I.F.T's and "Eleanor's" formats to obtain a unique payment solution.

[5] This means that the applications use "production-grade" certificates. At the time of writing, the 8 banks in the production phase are Deutsche Bank, HypoVereinsbank, Commerzbank, Bank of America, ABN Amro, Wells Fargo, Royal Bank of Scotland and Sanwa Bank.

- **FX-Trading with Continuous Linked Settlement (CLS)**

  ABN AMRO **[ABNA00]**, **[Iden01b]**, and Bank of America use Identrus certificates to secure the access to their CLS-application, which is used for the secure trading of foreign currencies.

- **Marketplace transactions in the Cargo Community Network**

  Deutsche Bank uses Identrus certificates in Singapore for trust-enabling and validating air-freight marketplace transactions at the Cargo Community Network **[CCNe01]** (see also **[Full01]**).

- **Corporate pension insurance sales**

  HypoVereinsbank **[Land01] [Iden01b]**, together with Allianz and Württemberger Hypo (a subsidiary of HVB), uses Identrus certificates for a web-based corporate pension insurance sales application.

- **IT-supply procurement platform**

  HypoVereinsbank **[Land01]** uses Identrus certificates within an IT-supply procurement platform in which customers, like Allianz for example, can order PC- and server products from Siemens.

These few examples show, that there are already existing real world applications for Identrus and, as can be seen from the last three examples, it is important for financial institutions to use (a network of) complementary partners to unleash the potential of Identrus in three- (and in the future also four-) corner applications.

5 Conclusion

In this paper we provided a brief overview of Identrus and focused on existing as well as potential future applications utilising this global trust infrastructure. This discussion shows that

- Identrus offers an outstanding strategic opportunity for financial institutions to reintermediate into the e-commerce value chain of its corporate customers
- there is a business case for Identrus deployment, where revenues from conscientiously chosen applications (bundled with new value adding services) compensate (even for high) investments in an Identrus infrastructure
- creating a tailor-made application roadmap is not a trivial, but - using the generic guidelines and general principles discussed in this work and external support by experienced people - a feasible task
- it needs to be stressed that the scope of Identrus-enabled applications is not at all limited to classical financial applications, such as payments, but covers the entire value chain of trading
- there are first real world Identrus-enabled applications in production and that this line of business represents a major potential for growth in the future.

References

[ABNA00] ABN Amro: *ABN AMRO settles on Identrus*, via http://www.etrendonline.com/glossary/ABN-AMR.asp

[AuOG98] Australian Office of Government - Information Technology: *Gatekeeper: A strategy for public key technology use in the Government*, 6 May 1998, via http://www.govonline.gov.au/publications/index.htm

[Bole01] Bolero International Ltd.: *Bolero Homepage*, via http://www.bolero.net

[CCNe01] CCNet: *Cargo Community Network Homepage*, via http://www.ccn.com.sg

[DeuB01] Deutsche Bank AG: *Electronic Bill Presentment Payment*, press release http://www.db.com/central/news/press_releases/2001/05022001b.htm

[Full01] Fullerton, I.: *The business case for Identrus*, talk at Identrus System Deployment Conference 2001, slides via http://www.secunet.com/identrus/

[Hühn01] Hühnlein, D.: *Identrus-enabled applications*, full and continuously updated version of the current paper, via http://www.secunet.com/identrus/

[Iden01a] Identrus LLC: *Identrus homepage*, at http://www.identrus.com

[Iden01b] Identrus LLC: *Case Studies*, via http://www.identrus.com/products/casestudies.xml

[Land01] Landsmann P.: *Global Trust - The HypoVereinsbank approach to trusted B2B eCommerce*, talk at Identrus System Deployment Conference 2001, slides via http://www.secunet.com/identrus/

[Maes01] Maes, J.: E-commerce solutions powered by banks, talk at Identrus System Deployment Conference 2001, slides via http://www.secunet.com/identrus/

[Mill01] Miller, L.: *Global systems and legal interoperability*, (reprinted abstract), eTrend, Issue 3, Spring 2001, page 32-33, or full version at http://www.e-comlaw.com

[PKCS7] RSA Laboratories: *PKCS #7 - Cryptographic Message Syntax Standard*, via http://www.rsalabs.com/pkcs/pkcs-7/index.html

[PKCS10] RSA Laboratories (Kaliski, B.): PKCS#10 - Certification Request Syntax Standard, Version 1.5, RSA-Laboratories, via http://www.rsalabs.com/pkcs/pkcs-10/index.html

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol*, via http://www.ietf.org

[Secu01] Secunet AG: *Identrus@secunet – Identrus from best source*, whitepaper, 2001, via http://www.secunet.com/identrus/

[Slog01] Slogar, A.: Trade facilitation on the internet, talk at Identrus System Deployment Conference 2001, slides via http://www.secunet.com/identrus/

[X.509] ITU-T Recommendation X.509: *Information Technology—Open Systems Interconnection—The Directory: Authentication Framework*, International Telecommunication Union, Geneva, Switzerland, 1997 (equivalent to ISO/IEC 9594-8)

Appendix – Identrus participants

The following list, which is compiled from press-releases available at **[Iden01a]**, comprises the participants in the Identrus initiative. The participants, who (as of May 2001) entered the production stage are printed **bold**.

- **April 1999**

  founded by **ABN AMRO**, **Bank of America**, Barclays PLC, Chase Manhattan, Citigroup, **Deutsche Bank**, (Bankers Trust now Deutsche Bank), **HypoVereinsbank**

- **September 1999**

  Industrial Bank of Japan, **Royal Bank of Scotland** joined

- **December 1999**

  Sanwa Bank, HSBC joined

- **April 2000**

  Australia and New Zealand Banking Group Limited (ANZ), Banco Santander Central Hispanol (BSCH, Spain), BNP Paribas (France), Caisse Nationale de Crédit Agricole (France), **Commerzbank**, Dresdner Bank, Scotiabank (Canada), Société Générale (France), **Wells Fargo & Company** (USA) joined

- **July 2000**

  Banco Bilbao Vizcaya Argentaria, S.A. (BBVA, Spain/Latin America), Bank of Scotland, ING Group (Benelux), Lloyds TSB (United Kingdom), National Australia Bank Limited, Royal Bank of Canada, The Sakura Bank Ltd. (Japan), The Sumitomo Bank Ltd. (Japan), Westpac Banking Corp. (Australia) joined

- **September 2000**

  partnership between S.W.I.F.T (owned by > 3000 banks) and Identrus

- **November 2000**

  MeritaNordbanken Unibank (Finland), SEB Bank (Sweden), WestLB (Germany), The Co-operative Bank (UK), Abbey National PLC (UK)

- **February 2001**

  AIB Group (Ireland), Bank of Ireland, The Bank of Tokyo-Mitsubishi Ltd., Banco Sabadell (Spain), Banesto (Spain), Crédit Lyonnais (France), The PNC Financial Services Group, Inc. (United States)

- **May 2001**

  Landesbank Baden Württemberg, DNB, Mizuho Group (Japan), Allied Irish, FleetBoston Financial Corporation (United States), Banco Comercial Portugues (Portugal)