SILVIA QUANDT
RESEARCH GMBH

RESEARCH

OPENLIMIT AG – TAKING YOUR SIGNATURE INTO THE DIGITAL ERA

_DIGITAL SIGNATURES ARE COMING

_NEED FOR AUTHENTICATED DOCUMENTS ARE RISING

_OPENLIMIT IS BEST POSITIONED TO PROFIT FROM THE ABOVE TRENDS

_BUY RECOMMENDATION, FAIR VALUE € 4.20

Jacques Abramowicz, Head of Technology, Media and Telecommunications
16 September 2009

Contents

OpenLimit AG

Headquarter
Zugerstrasse 76b
6341 Baar
Switzerland

IR
Marc Gurov
ir@openlimit.com
www.openlimit.com
Phone +41 (0)41 / 560 10 20

Stock data

Main Market
MDAX, General Standard

Symbol
O5H.DE (Reuters)
05H:GR (Bloomberg)

Market cap.
€ 24.42 m
(note: market cap in € not CHF)

No. of outstanding shares
16.767 m common

Indices
General Standard

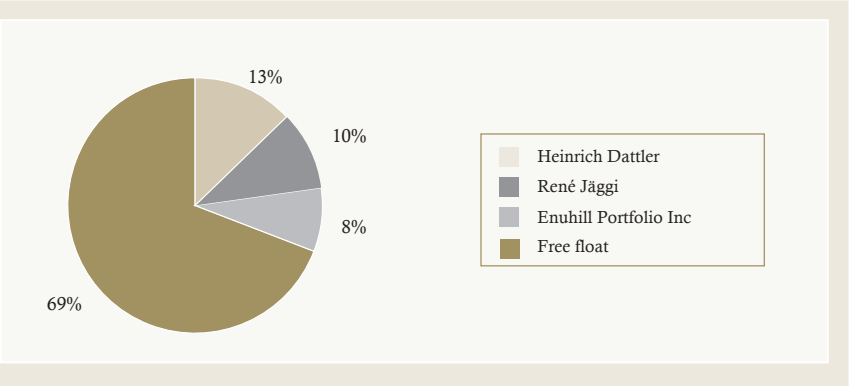
Next Event
Q3 results 7 November 2009

Free Float
68,07 %

CHF m	*2008*	*2009e*	*2010e*	*2011e*	*2012e*
Revenues	7,137,945	8,360,000	10,706,918	15,400,000	25,400,000
Total Income	9,282,269	10,718,756	13,280,106	18,275,000	28,387,500
EBITDA	3,158,207	4,277,218	6,480,106	11,008,000	20,566,000
EBIT	2,036,758	3,091,682	5,257,106	9,663,000	19,111,000
Profit	1,602,095	2,867,752	5,175,606	9,640,000	15,030,879
EPS	0.10	0.17	0.31	0.57	0.89
Employees	46	53	62	70	76

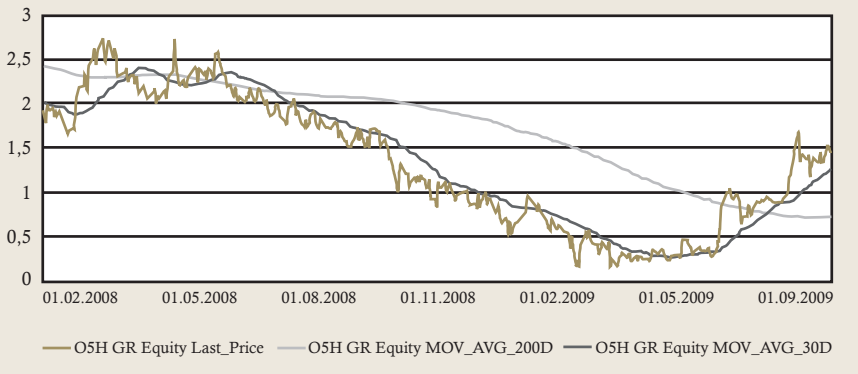
Source: OpenLimit AG, Silvia Quandt Research GmbH

Shareholder Structure



Source: Silvia Quandt Research GmbH, Company Data

Company Share Price Developement



Source: OpenLimit AG, Silvia Quandt Research GmbH, Bloomberg, Prices as of 01.09.2009

Key Messages to take from this Note

Digitalisation is changing our lives in every way possible, but it is currently very difficult to sign contracts or do business with the government or other institutions. A legally recognised digital signature could change this and simplify our lives.

OpenLimit is well ahead of the field when it comes to digital signatures, digital document signing or authenticating archived documents.

We believe that the approval of the German Bundestag on 19 December 2008, to introduce an electronic identity card by November 2010 can be the big breakthrough that this industry has been waiting for and will show why OpenLimit is well placed to profit.

We see enormous potential in OpenLimit's MigSafe product as we believe that digital storage, once secure and manipulation free, will take off as a mass market by corporations trying to cut down on costs. The savings of physical storage make the investment in the software look pale in comparison.

In Belgium the Government has succeeded in introducing over 10 million eID cards in a short while. This bodes well for OpenLimit's efforts in Germany, which is a much greater market.

OpenLimit AG

About OpenLimit AG

OpenLimit stands out with its highly advanced development and marketing of customer-orientated, reliable and internationally certified signature software. OpenLimit also provides customer support with specialist expertise and the best possible service partnership synergies.

OpenLimit collaborates closely with renowned partners such as Adobe Systems, CSC, Fujitsu Technology Solutions, Ingram Micro, Microsoft, Sun Microsystems, Deutscher Sparkassenverlag and Swisscom Solutions. Adobe Systems has developed the „intelligent PDF file" with an integrated field for generating signatures. In addition to other multimedia contents, a certified electronic signature can be generated in online forms using the OpenLimit signature software. This is legally accorded the same status as the handwritten signature in the member states of the European Union, Switzerland and many other countries.

The OpenLimit security technologies comprise universally applicable signature software with encryption functionality, which is currently the only solution world-wide to have been certified in compliance with the Common Criteria EAL4+. The OpenLimit document technologies incorporate a PDF, PDF/A and TIFF producer and allow the user to merge or repair PDF documents. The archive technologies from OpenLimit supplement archiving solutions taking into consideration legally compliant and audit-secure, long-term archives.

As well as implementation, consulting and training services, OpenLimit offers allround, support services throughout Europe for all its products through its partner, Fujitsu Technology Solutions. The customer can call a toll-charge hotline, purchase a support package for one year or sign a software maintenance agreement.

Management Team

Marc Gurov, CEO

Marc Gurov was born in 1973 and is a US national. He attended school in Germany and the United States. He studied international business at Florida Atlantic University in Boca Raton, Florida, U.S.A. After graduating, Mr. Gurov worked in the United States for various companies on a freelance basis with the main focus on marketing and consulting. Since 2009 he is the CEO.

Dirk Arendt

Dirk Arendt was born in 1966 and is a German national. As Vice President, Business Development, he has been a member of the board of management of the OpenLimit Group since January 2009. In 2002 Dirk Arendt started working for the Fraunhofer Gesellschaft e.V. There he has been establishing and developing the business area „eGovernment" as scientific assistant at the Fraunhofer Institute FOKUS. Dirk Arndt is one of the co-initiators and „driving force" of the idea of the „independent Fraunhofer FOKUS eGovernment laboratory. Dirk Arndt represents the interests of OpenLimit in selected national and international boards and associations.

Armin Lunkeit

Armin Lunkeit was born in 1978 and is a German national. As Chief Development Officer, he has been a member of the board of management of the OpenLimit Group since December 2007. He studied microsystems technology at the Technical College of Technology and Economics in Berlin, from where he graduated in 2002 as a chartered engineer. Mr. Lunkeit entered the field of software development in 2000. After concluding his studies, he worked as a developer for Kithara GmbH. Mr. Lunkeit worked at OpenLimit SignCubes GmbH in product development from June 2003 until he took over his present position.

Reinhard Stüber

Reinhard Stüber was born in 1952 and is a German national. As Senior Vice-President, New Business Development, he is a member of the board of management of the OpenLimit Group. He studied engineering sciences (chartered engineer) at the Engineering College of Water Resources Management in Magdeburg, Germany concentrating on hydraulic engineering. From 1973 to 1993 he worked for various German companies as an engineer. Between 1993 and 2001 he was in charge of the Software department at UVE GmbH. He took over the position of Business Development Manager at OpenLimit SignCubes AG in 2001.

Ronny Wittig

Ronny Wittig was born in 1978 in Germany. As Chief Sales Officer, he has been a member of the Board of Management at OpenLimit AG since April 2009. He finished his vocational training as management assistant in IT systems at the Deutsche Telekom Group and then worked for various companies. He had successfully held the position of Business Development and Project Manager for several years at the PC-Ware Information Technologies AG. Moreover, he developed significant strategic product and service portfolios for software producers. Since 2007 Ronny Wittig has been in charge of the Sales department at OpenLimit AG.

Digital Signature Market

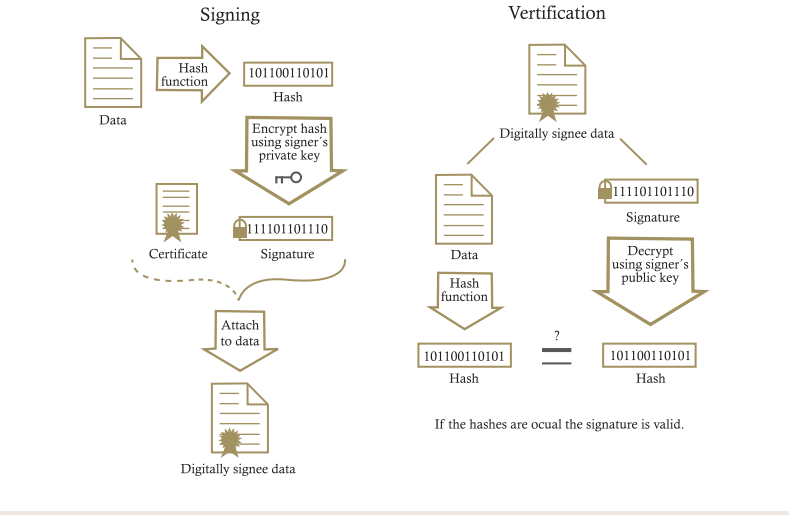
The Digital Signature Algorithm (DSA) is a United States Federal Government standard or FIPS for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS), and adopted in 1993.

DSA is covered by U.S. Patent 5,231,668, filed 26 July, 1991, and attributed to David W. Kravitz, a former NSA employee. This patent was given to „The United States of America as represented by the Secretary of Commerce, Washington, D.C." and the NIST has made this patent available world-wide royalty-free.

A digital signature or digital signature scheme is a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything representative as a bitstring: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States and the European Union, electronic signatures have legal significance. However, laws concerning electronic signatures do not always make clear whether they are digital cryptographic signatures in the sense used here, leaving the legal definition, and so their importance, somewhat confused.

In the famous paper "New Directions in Cryptography" (1976), Whitfield Diffie and Martin Hellman first described the notion of a digital signature scheme, although they only conjectured that such schemes existed. Soon afterwards, Ronald Rivest, Adi Shamir, and Len Adleman invented the RSA algorithm that could be used for primitive digital signatures. (Note that this just serves as a proof-of-concept, and "plain" RSA signatures are not secure.) The first widely marketed software package to offer digital signature was Lotus Notes 1.0, released in 1989, which used the RSA algorithm.



Source: Silvia Quandt Research GmbH

Benefits of digital signatures

Below are some common reasons for applying a digital signature to communications:

Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as non-malleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible.

Drawbacks of digital signatures

Despite their usefulness, digital signatures alone do not solve the following problems:

Association of digital signatures and trusted time stamping

Digital signature algorithms and protocols do not inherently provide certainty about the date and time at which the underlying document was signed. The signer might have included a time stamp with the signature, or the document itself might have a date mentioned on it. Regardless of the document's contents, a reader cannot be certain the signer did not, for example, backdate the date or time of the signature. Such misuse can be made impracticable by using trusted time stamping in addition to digital signatures.

Non-repudiation

In a cryptographic context, the word repudiation refers to any act of disclaiming responsibility for a message. A message's recipient may insist the sender attached a signature in order to make later repudiation more difficult, since the recipient can show the signed message to a third party (e.g. a court) to reinforce a claim as to its signatories and integrity. However, loss of control over a user's private key will mean that all digital signatures using that key, and so ostensibly 'from' that user, are suspect. Nonetheless, a user cannot repudiate a signed message without repudiating their signature key. This is aggravated by the fact there is no trusted time stamp, so new documents (after the key compromise) cannot be separated from old ones, further complicating signature key invalidation. A non-repudiation service requires the existence of a public key infrastructure (PKI) which is complex to establish and operate. The certificate authorities in a PKI usually maintain a public repository of public keys so the associated private key is certified and signatures cannot be repudiated. Expired certificates are normally removed from the repository. It is a matter for the security policy and the responsibility of the authority to keep old certificates for a period of time if non-repudiation of data service is provided.

WYSIWYS

Technically speaking, a digital signature applies to a string of bits, whereas humans and applications "believe" that they sign the semantic interpretation of those bits. In order to be semantically interpreted the bit string must be transformed into a form that is meaningful for humans and applications, and this is done through a combination of hardware and software based processes on a computer system. The problem is that the semantic interpretation of bits can change as a function of the processes used to transform the bits into semantic content. It is relatively easy to change the interpretation of a digital document by implementing changes on the computer system where the document is being processed. From a semantic perspective this creates uncertainty about what exactly has been signed. WYSIWYS (What You See Is What You Sign) means that the semantic interpretation of a signed message can not be changed. In particular this also means that a message can not contain hidden info that the signer is unaware of, and that can be revealed after the signature has been applied. WYSIWYS is a desirable property of digital signatures that is difficult to guarantee because of the increasing complexity of modern computer systems.

Additional security precautions

Putting the private key on a smart card

All public key / private key cryptosystems depend entirely on keeping the private key secret. A private key can be stored on a user's computer, and protected by a local password, but this has two disadvantages:

__ the user can only sign documents on that particular computer
__ the security of the private key depends entirely on the security of the computer

A more secure alternative is to store the private key on a smart card. Many smart cards are designed to be tamper-resistant (although some designs have been broken, notably by Ross Anderson and his students). In a typical digital signature implementation, the hash calculated from the document is sent to the smart card, whose CPU encrypts the hash using the stored private key of the user, and then returns the encrypted hash. Typically, a user must activate his smart card by entering a personal identification number or PIN code (thus providing two-factor authentication). It can be arranged that the private key never leaves the smart card, although this is not always implemented. If the smart card is stolen, the thief will still need the PIN code to generate a digital signature. This reduces the security of the scheme to that of the PIN system, although it still requires an attacker to possess the card. A mitigating factor is that private keys, if generated and stored on smart cards, are usually regarded as difficult to copy, and are assumed to exist in exactly one copy. Thus, the loss of the smart card may be detected by the owner and the corresponding certificate can be immediately revoked. Private keys that are protected by software only may be easier to copy, and such compromises are far more difficult to detect.

Using smart card readers with a separate keyboard

Entering a PIN code to activate the smart card commonly requires a numeric keypad. Some card readers have their own numeric keypad. This is safer than using a card reader integrated into a PC, and then entering the PIN using that computer's keyboard. Readers with a numeric keypad are meant to circumvent the eavesdropping threat where the computer might be running a keystroke logger, potentially compromising the PIN code. Specialized card readers are also less vulnerable to tamper with their software or hardware and are often common criteria EAL3 certified.

Other smart card designs

Smart card design is an active field, and there are smart card schemes which are intended to avoid these particular problems, though so far with little security proofs.

Using digital signatures only with trusted applications

One of the main differences between a digital signature and a written signature is that the user does not "see" what he signs. The user application presents a hash code to be encrypted by the digital signing algorithm using the private key. An attacker who gains control of the user's PC can possibly replace the user application with a foreign substitute, in effect replacing the user's own communications with those of the attacker. This could allow a malicious application to trick a user into signing any document by displaying the user's original on-screen, but presenting the attacker's own documents to the signing application.

To protect against this scenario, an authentication system can be set up between the user's application (word processor, email client, etc.) and the signing application. The general idea is to provide some means for both, the user app and signing app, to verify each other's integrity. For example, the signing application may require all requests to come from digitally-signed binaries.

Administration Client

The German government intends to introduce new identity cards (eID) capable of carrying a digital signature in November 2010 to all legitimate citizens. Starting in October there will be a test involving 30 companies to enable them to conduct online business within a legal and recognised framework.

To achieve this, the German government intends to introduce a citizen client to use the eID functionality of these new identity cards. Companies bidding to deliver this client need to have fully functional software running by 31 October 2010 and also need to provide an eID-Service, which is a server product used by companies and government agencies to authenticate eIDs.

This probably surprised some companies pitching for the deal since not only the client but also the processes behind it are needed. Submissions to the German government had to be submitted by 30 June 2009. The government wanted at least 5 bidders and maximum of 8 in this limited tender. We doubt that 5 consortia can be found.

OpenLimit naturally pitched for the client. Having previously worked together with Fujitsu Technology Solutions, Deutsche Telekom, the Bundesdruckerei and Microsoft, OpenLimit has the advantage that its software client is already developed and out in the market. Furthermore, according to our understanding, the OpenLimit client carries the seal of approval of the Federal Office for Information Security (BSI - Bundesamt für Sicherheit in der Informationstechnik).

The only other company claiming to have a client available is **Bremen online services** (bos) a company founded by subsidies of the Federal Ministry of economics and technology (BMWi) whose project used to be called Media@KOMM.

Another contender to deliver the administration client is **Giesecke & Devrient** (G&D), Germany's second biggest producer of security- and chipcard-appliances. G&D needs to be successful having lost out on both the German Passport and new identity card production. Through its secunet subsidiary, G&D has been working closely with the BSI on cryptology which may help it in pitching.

The forth company pitching is industry heavyweight **IBM** who definitely has the capability of developing the necessary client.

The problem for all parties pitching for the administration client they not only have to present a solution but to also deliver a proposal. Note that the client (eID software) did not necessarily have to have completed the certification process in order to pitch.

Sales by Products

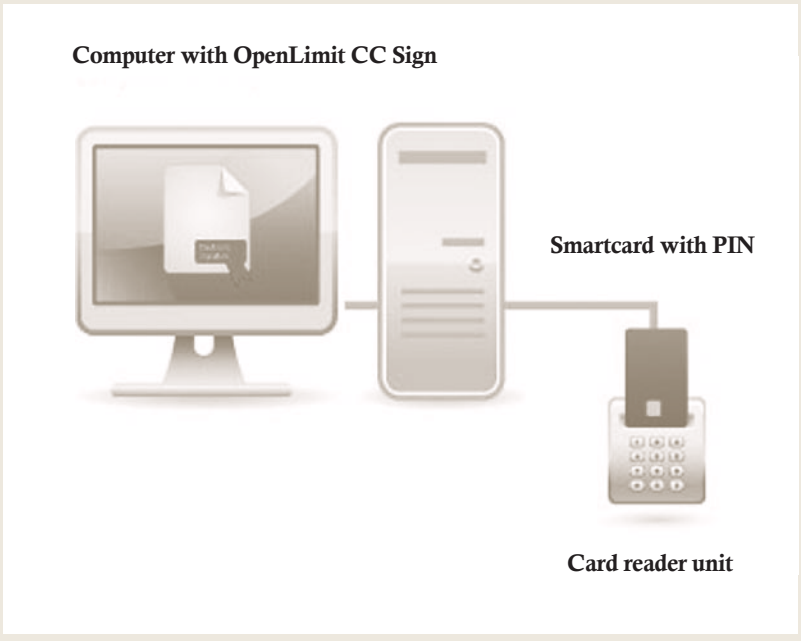
OpenLimit has three main product lines:

__Security Technologies
Client
Integration and Server
Products for Form Server

__Document Technologies

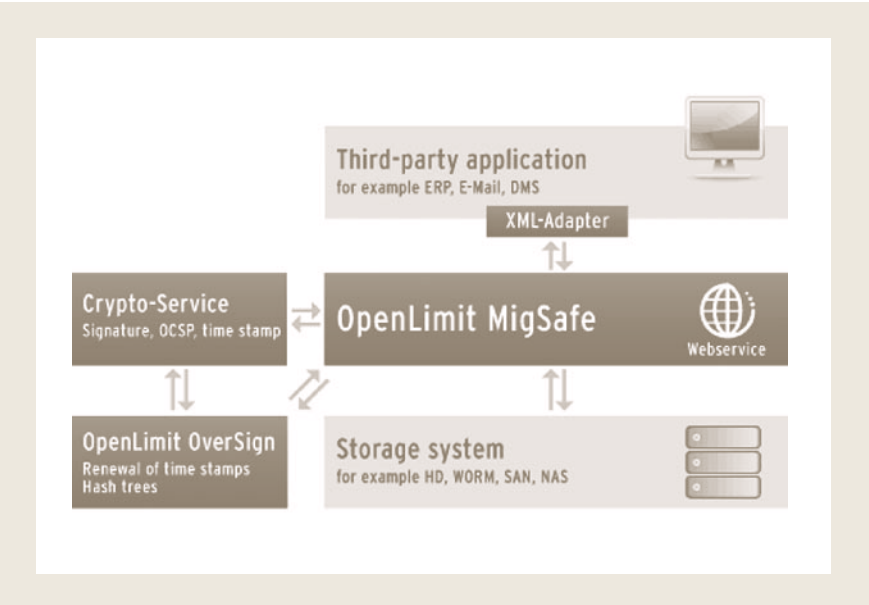
__Technologies for eArchives

OpenLimit CC Sign and its derivatives can be used to generate qualified or advanced electronic signatures, if necessary even directly in Adobe Reader or Acrobat as well as Microsoft, Lotus Notes and most commonly used browsers. It can also be used to verify the validity of existing signatures. Documents can simply be signed with a mouse-click and converted into PDF/A format for long-term archiving purposes.



Source: OpenLimit AG

OpenLimit MigSafe is an overall middleware solution. It allows customers to move files from any specialist application to a suitable storage medium with the MigSafe middleware. The technology relies on a globally deployable Web service technology and XML-based document containers with unique identification numbers. This will guarantee loss-free migration of digital archives in the future – thus electronic documents will still be readable in 100 years.



Source: OpenLimit AG

SWOT Analysis

Strengths

__Strong links to industry standards such as Microsoft and Adobe

__Strong and diversified product portfolio.

Weaknesses

__Market still small and fragmented. A lot of upfront investments needed for Europe wide (global) certification

Opportunities

__Nearly limitless. From legal emails to contracts, from doing business with local authorities to secure shopping on the internet.

__With an electronic identification card on the programme of several European governments and new forms of digital health cards.

__Corporations can assure that documents sent and received are not manipulated. The same goes for emails.

__Long-term archiving

Threats

__Microsoft could decide to purchase a technology and integrate it into future operating systems moving away from its current position of just providing the infrastructure around these products.

__The DSA algorithm could be hacked faster than it is constantly evolving, making it worthless.

__Government near organisations like Belgian Certipost could use government influence to establish themselves as a standard.

Regulation

EU Governments are trying to force the speedy introduction of digital signatures

On 28 November 2008 the European Commission adopted an "Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market".

Efficient eSignatures for easier access to online public services

Public authorities offer more and more public services by electronic means. They are also increasingly allocating and conducting government contracts through online procedures. Until now the implementation focused mainly on national needs and means. Because of this national focus, companies and individuals from an EU country had limited access to these online public services in another EU country, 'e-barriers' appeared to hamper a well-functioning Single Market.

The Action Plan seeks an EU-wide solution to cross-border use of online public services. It is committed to quick delivery and results.

Efficient cross-border public services require the mutual recognition and interoperability of electronic signatures and identification solutions. The Action Plan will help Member States to implement these solutions and focuses mainly on e-government applications. However, its recommendations can also be used in Business to Business (B2B) and Business to Consumers (B2C) transactions.

In the framework of the Lisbon Strategy, the EU has committed itself by improving the legal and administrative environment to unlock business potential. Bringing public administrations on line, and enabling enterprises and individuals to communicate electronically with public administrations across borders, contributes to create an environment that favours entrepreneurship and facilitates citizen's contact with public authorities.

Electronic communications are becoming increasingly important in many aspects of economic and public life. Public authorities across Europe have started to offer electronic access to government services. In doing so they have been focusing mostly on national needs and means, which have led to a complex system with different solutions. This situation carries the risk of creating new barriers to cross-border markets and of hampering the functioning of the single market for enterprises and citizens.

Major barriers to cross-border access to electronic services of public administrations are linked to the use of electronic identification and of electronic signatures. Like in the non-digital environment, certain electronic procedures may require identification and signatures. Thus access to public administrations electronic procedures often implies the need for the individuals involved to identify themselves (i.e. allowing the administration to make sure that the persons are who they claim to be by checking their personal credentials) and the need to provide an electronic signature allowing the administration to identify the signatory as well as to make sure that the data submitted has not been altered during transmission). The main barrier is the lack of interoperability, be it legal, technical or organisational.

The current European Union framework offers horizontal and sectoral instruments to facilitate and enhance the use of e-signatures and e-identification. The e-signatures

Directive establishes the legal recognition of electronic signatures and a legal framework to promote their interoperability. A number of practical, technical and organisational requirements need to be met to establish such interoperability.

Furthermore, effective interoperability is also required if Member States are to comply with their legal obligations under other EU legislation, in particular under specific internal market instruments. Several internal market initiatives foresee that businesses should be able to use electronic means to communicate with public bodies, exercise their rights and do business across borders.

The Services Directive obliges Member States to ensure by the end of 2009 that service providers are able to complete electronically and at a distance all procedures and formalities necessary to provide a service activity. This implies, amongst other things, the possibility for cross-border identification of service providers and authentication of the data submitted.

The Directives on Public Procurement aim to promote the development and use of electronic means in public purchasing procedures, with potentially substantial cost savings for business. Member States may regulate the level of electronic signature required in line with the obligations of the e-Signatures Directive, and may restrict the choice of contracting authorities to qualified signatures.

Electronic invoicing – the electronic transfer of invoicing information (billing and payment) between business partners (supplier and buyer) – is an essential part of an efficient financial supply chain. To accompany the creation of Single Euro Payment Area, work is under way to prepare an e-invoicing initiative (the European Commission has set up an expert group tasked with establishing a European Electronic Invoicing Framework by 2009) with further savings for businesses.

The objective of this Action Plan is therefore to offer a comprehensive and pragmatic framework to achieve interoperable e-signatures and e-identification, which will simplify access of enterprises and citizens to cross-border electronic public services. To achieve this objective, the Action Plan focuses on a number of practical, organisational and technical issues, complementing the existing legal framework.

Current framework for e-signatures and e-identification at EU level

The e-Signatures Directive

The e-Signatures Directive was adopted in 1999 to promote the legal recognition of electronic signatures and to ensure the free circulation within the single market of e-signature products, equipment and services. However, a legal and technical analysis of the practical usage of e-signatures shows that there are interoperability problems that currently limit the cross-border use of e-signatures. The analysis highlights the need for a more effective mutual recognition approach. Fragmentation due to the lack of cross-border interoperability is likely to affect e-government services in particular, which today are the largest channel of transactions using e-signatures.

The i2010 e-Government Action Plan

With regard to cross-border e-identification, there is still no community instrument on which action at community level could be based. Notwithstanding this, the Commission supports (both politically and financially) activities that aim at finding solutions to interoperable e-identification at EU level. In this regard, the i2010 e-Government Action Plan, adopted by the European Commission on 25 April 2006, considers interoperable electronic identity management (eIDM) as one of the critical key enablers for access to public services. The importance of interoperable eIDM has been recognised by the Member States who have made the clear commitment to ensure that "by 2010 European citizens and businesses will be able to benefit from secure and convenient electronic means, issued at local, regional or national levels and complying with data protection regulations, to identify themselves to public services in their own or in any other Member State".

Enhancing the cross-border interoperability of e-signatures and e-identification

Despite the existing legal provisions and the political commitments taken by the Member States and the Commission, a more coordinated and comprehensive approach is needed to facilitate the cross-border use of e-identification and e-signatures in practice. This is essential to avoid fragmentation of the single market.

Therefore, the Commission proposed in its Communication "A single market for the 21st century Europe" of 20 November 2007 to adopt an Action Plan on e-signatures and e-authentication.

This Action Plan aims to assist Member States in implementing mutually recognised and interoperable electronic signatures and e-identification solutions, in order to facilitate the provision of cross-border public services in an electronic environment. It sets out specific actions on e-signatures (part 1) and on e-identification (part 2). Although the Action Plan focuses mainly on e-government applications, the suggested actions will also benefit businesses' applications insofar as the means to be put in place can also be used in Business to Business (B2B) and Business to Consumers (B2C) transactions.

At the Spring European Council of March 2008, Heads of State or Government declared that it is crucial to put in place cross-border interoperable solutions for electronic signatures and e-authentication to improve the functioning of the 'e-Single Market'.

The Commission will contribute to develop a coordinated response to interoperability issues by monitoring progress and giving guidance to Member States and stakeholders on the implementation of the Action Plan.

Electronic signatures as a legal concept

In European legislation the term "electronic signature", is defined as follows:
"data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication".

This definition is deliberately very wide and doesn't refer to any technological or security-related requirements. As a consequence, simply adding the sender's name at the bottom of an email is, from a legal point of view, considered as an electronic signature. Would this email (or a paper copy of it) be presented in a litigation procedure as a piece of evidence, the court could take it into account, at least if nobody is contesting its authenticity. As a consequence, all kinds of electronic signatures, in the widest sense, have a potential legal validity.

This doesn't mean that any kind of electronic signature will be considered legally valid in all circumstances. For example in Belgium, in order to be accepted as a legal piece of evidence, a contract in electronic form requires a signature by which the origin of the signatory and the integrity of the contents of the contract can be controlled. Other example: the European and Belgian laws accept electronically signed invoices under the condition that they are secured by means of advanced electronic signatures (see further). In some cases the law will require the use of advanced electronic signatures based on qualified certificates and/or created by means of a secure device. Other laws explicitly require electronic signatures to be created by means of the Belgian electronic identity card or any equivalent technique.

The question whether an electronic signature is legally valid or not, can therefore not be answered with a "yes" or "no". The legal validity will always have to be examined in the perspective of a particular context.

The term "electronic signature" relates to data authentication and does not refer to entity authentication. For example, entering a PIN-code and/or a one-time challenge to get access to an electronic bank account will not fall within the scope of the "electronic signature" definition. Entering the same code in order to confirm a financial transaction, on the contrary, is an example of data authentication and is therefore considered as an electronic signature. As a consequence, an identical action (entering a PIN) will, depending on the context, be considered as a signature or not.

Advanced electronic signatures

Also known as qualified electronic signatures, this is the area OpenLimit focuses on

More and more legal rules refer to advanced electronic signatures. An advanced electronic signature, as defined in the European legislation, is an electronic signature meeting each of the following four requirements:

- it is uniquely linked to the signatory
- it is capable of identifying the signatory
- it is created using means that the signatory can maintain under his sole control
- and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

These requirements are formulated in a general and technology-neutral way. As far as the law is concerned, these abstract requirements can theoretically be filled out by any imaginable technical solution. How – by means of which technological solution – the four requirements are complied with, is irrelevant for the legislator. In practice however, the definition refers to electronic signatures based on digital signature technology, making use of public key cryptography. Everybody agrees that this technology is currently the only one which can meet all of the four requirements.

Qualified certificates

This area is covered by OpenLimit's CC-Sign

A certificate is legally defined as "an electronic attestation which links signature-verification data to a person and confirms the identity of that person". The term "signature-verification data" is the legal term for public key.

Certificates are often called digital IDs because, like identity cards, they are issued by a trusted authority to a person whose identity has first been controlled. The certificate is secured by means of a digital signature allowing the verification of its origin and its integrity.

The value of a certificate is very much dependent of two factors: the reputation of the certificate issuer – the CSP – and the quality of the registration procedure. During the registration procedure, the CSP controls the identity of the certificate applicant. This control is crucial because the certificate issued by the CSP will confirm that the public key mentioned in the certificate, belongs to the person identified in this certificate.

The European legislation contains the notion of a "qualified certificate". This is a certificate that meets certain formal requirements and which is issued by a "qualified CSP". In some particular cases, the law requires electronic signatures supported by qualified certificates. The formal requirements of a qualified certificate are listed in Annex 1 of the European Directive (and have literally been copied in Annex 1 of the Belgian law). According to this Annex qualified certificates must contain:

- an indication that the certificate is issued as a qualified certificate
- the identification of the CSP and the State in which it is established
- the name of the signatory or a pseudonym, which shall be identified as such
- provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended
- signature-verification data which correspond to signature-creation data under the control of the signatory
- an indication of the beginning and end of the period of validity of the certificate
- the identity code of the certificate
- the advanced electronic signature of the CSP issuing it
- limitations on the scope of use of the certificate, if applicable
- and limits on the value of transactions for which the certificate can be used, if applicable.

The ETSI Technical Specification (TS 101 862) defines how the X.509 public key certificate format, which dominates the public key infrastructure market, may be used to meet the requirements of Annex I of the Directive. In addition, where there is currently no defined mechanism for meeting a requirement (e.g. limits on the value of the transaction) the specification builds on the existing extension capabilities of X.509 to define the necessary optional data structures.

Besides the formal requirements listed above, a qualified certificate has to be issued by a qualified CSP. A CSP is qualified if he complies with a series of security requirements, which are listed in Annex 2 of the European Directive (Annex 2 of the Belgian law). These requirements relate to the financial stability, the quality of the personnel, the security measures taken, etc. If a CSP claims to issue qualified certificates to the public, he has to notify this to the public authority and he will subsequently operate under the supervision of this authority.

Qualified electronic signatures

This area is covered by OpenLimit's CC-Sign

The European Directive and other European law attribute to so-called qualified electronic signatures, in relation to electronic data, the same status as handwritten signatures have in relation to paper documents. Qualified electronic signatures are advanced electronic signatures based on a qualified certificate and created by means of a secure signature-creation device.

The assimilation of qualified electronic signatures to handwritten signatures doesn't mean to require the use of qualified electronic signatures in every situation in which, up to now, the use of handwritten signatures was obligatory. Traditional procedures based on the use of paper documents and handwritten signatures are often replaced by electronic processes including all sorts of technical and organizational security measures. These processes do not always necessarily have to include the use of electronic signatures.

In many situations however, our activities are still regulated by old legal provisions. These provisions refer, sometimes explicitly but very often implicitly, to the use of paper documents and handwritten signatures. In such cases, the question arises if the use of electronic signatures is at all permitted. This is where the qualified electronic signature comes in. Even if the law doesn't mention the possibility of using electronic signatures, the use of a qualified electronic signature will always be considered having the same value as a handwritten signature. As a consequence there are two possibilities. Either the law explicitly defines the type of electronic signature required in a particular context: in this case the legal provisions have to be complied with. Or the law merely requires – explicitly or implicitly – a document to be "signed": in this latter case a qualified electronic signature will automatically be considered having the same value as a handwritten signature. The principle just described is not only valid in Germany but in every Member State of the European Union. As a consequence, a German qualified electronic signature will have to be equated with a handwritten signature in every other EU country.

eID middleware

Specific middleware intended to be used together with the card has been developed and the source code has been made publicly accessible. The middleware is necessary for the interaction between the eID card and the application on the user's computer. Before using the eID card for the creation of electronic signatures, the user needs to download and install the middleware on his/her computer. In Germany the eID middleware should permit online authentication.

The middleware is implemented into each specific application by bridging between the applications itself and the device actually performing the cryptographic operations (the eID card, in conjunction with the compatible card readers). It consists out of two independent interface implementations.

For Microsoft standard applications, a so-called Cryptographic Service Provider implements the cryptographic operations from the smartcard. An application calls this implementation through a standard interface called Crypto API. This API enables application developers to add authentication, encoding, and encryption to their Win32-based applications. Application developers can use functions in the CryptoAPI without knowing anything about the underlying implementation, in much the same way as they can use a graphics library without knowing anything about the particular graphics hardware configuration. The middleware establishes the link between the abstract CryptoAPI and the underlying PKCS#11 interface.

Secondly, typically in non-Microsoft applications, the PKCS#11 (v2.11) interface is used. Custom applications can also make use of this interface instead of the CryptoAPI interface. The PKCS#11 interface is sometimes also called Cryptoki.

If a signature is requested with the signature key, the middleware will show a user interface to either ask the user to enter a PIN, or ask the user to supply a PIN at the PIN pad reader. Noteworthy is that the Belgian eID card currently uses one PIN for accessing the authentication and the signature key.

Signing self-authored documents

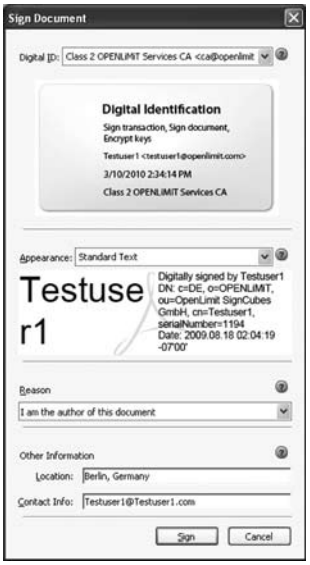
This area is covered by OpenLimit's CC-Sign

In a stand-alone context, Acrobat Standard or Professional enables a single user to create electronic signatures on self-authored documents (for example a letter created in Microsoft Word and saved as a PDF).

The first action to be taken by a document creator who opens the signature capability is to create a signature field. The signature field determines the location of the signature appearance on the document. It will obviously in most of the cases be created at the bottom of the document (see picture below).

The Adobe (or other) components deliver the document to the signature-middleware. The middleware calculates a hash-value and generates a signature with the external signature card.

Once the signature has been created by the eID, it will again be collected by the Adobe software and embedded in the document. Adobe's signature software acts, in other words, as a facilitator for electronic signatures. It facilitates the signing process by invoking the signature mechanism which further relies on the particular signing solution used (e.g. the signing technology of the German eID).



Source: OpenLimit AG

Financials

Income Statement

CHF m	*2008*	*2009e*	*2010e*	*2011e*	*2012e*
Revenue	7,137,945	8,360,000	10,706,918	15,400,000	25,400,000
add S/W development	2,144,324	2,358,756	2,573,188	2,875,000	2,987,500
Total Income	**9,282,269**	**10,718,756**	**13,280,106**	**18,275,000**	**28,387,500**
Cost of goods sold	0	98,000	150,000	120,000	170,000
Personnel expenses	4,554,969	4,720,123	4,950,000	5,250,000	5,650,000
Depreciation	1,121,449	1,185,536	1,223,000	1,345,000	1,455,000
Operational expenses	1,569,093	1,623,415	1,700,000	1,897,000	2,001,500
Income from Operations	**2,036,758**	**3,091,682**	**5,257,106**	**9,663,000**	**19,111,000**
Financial income	47,475	37,500	1,500	22,000	45,000
Financial expense	447,332	224,875	45,000	2,500	1,000
Income before taxes	**1,636,901**	**2,904,307**	**5,213,606**	**9,682,500**	**19,155,000**
Taxes	34,806	36,555	38,000	42,500	4,124,121
Net Income	**1,602,095**	**2,867,752**	**5,175,606**	**9,640,000**	**15,030,879**
Dividend paid	0	0	1,000,000	4,000,000	7,000,001
Net income after dividends	**1,602,095**	**2,867,752**	**4,175,606**	**5,640,000**	**8,030,878**
Shares outstanding	15,757,412	16,797,412	16,797,413	16,797,412	16,797,413
DPS	0.00	0.00	0.06	0.24	0.42
EPS	0.10	0.17	0.31	0.57	0.89

Source: Silvia Quandt Research GmbH, Company Data

Balance Sheet

CHF m	*2008*	*2009e*	*2010e*	*2011e*
Receivables	5,436,250	6,967,191	8,632,069	10,051,250
Cash and equivalents	101,435	-416,071	873,045	6,183,430
Current Assets	**5,537,685**	**6,551,120**	**9,505,113**	**16,234,680**
Intangible Assets	3,598,183	5,757,093	6,908,511	8,290,214
Plant & Equipment	141,658	155,250	205,736	155,250
Non-current Assets	**3,739,841**	**5,912,343**	**7,114,247**	**8,445,464**
Total Assets	**9,277,527**	**12,463,463**	**16,619,361**	**24,680,143**
Share capital	4,727,224	5,039,224	5,039,224	5,039,224
Share premium	7,876,218	9,024,968	9,024,968	9,024,968
Accumulated profit (loss)	-3,989,371	-1,121,619	3,053,987	8,693,987
Equity	**8,614,071**	**12,942,573**	**17,118,179**	**22,758,179**
Accounts payable	658,631	558,354	1,232,657	2,324,019
Tax liabilities	4,825	0	325,743	585,552
Current liabilities	**663,456**	**558,354**	**1,558,400**	**2,909,571**
Total equity & liabilities	**9,277,527**	**13,500,927**	**18,676,579**	**25,667,750**

Source: Silvia Quandt Research GmbH, Company Data

Cash Flow Statement

CHF m	*2008*	*2009e*	*2010e*	*2011e*
PAT	**1,602,095**	**2,867,752**	**5,175,606**	**9,640,000**
Depreciation & Amortisation	1,121,449	1,185,536	1,223,000	1,345,000
other provisions				
Cash Flow	**2,723,544**	**4,053,288**	**6,398,606**	**10,985,000**
change in receivables	1,676,692	3,703,443	2,866,782	2,750,397
Operating Cashflow	**1,676,692**	**349,845**	**3,531,824**	**8,234,603**
Capex	-2,258,551	-2,679,536	-1,725,202	-3,213,333
Acquisitions	0	0		
Investments (financial)	43,557	0		
Sales of tangible Assets				
Investment Cashflow	**-2,214,994**	**-2,679,536**	**-1,725,202**	**-3,213,333**
change in debt				
Dividend (previous year)	0	0	0	-1,000,000
Purchase of own shares				
change in capital		1,460,750		
other	-440,174	250,000		
Financial Cashflow	**-440,174**	**1,710,750**	**0**	**-1,000,000**
Liquidity change	-978,476	-618,941	1,806,622	4,021,269
Cash Position	**101,435**	**-517,506**	**1,289,116**	**5,310,385**

Source: Silvia Quandt Research GmbH, Company Data

Discounted Cash Flow

CHF m		*2007*	*2008*	*2009e*	*2010e*	*2011e*
Sales		4,847,070	7,137,945	10,706,918	15,400,000	25,400,000
EBITDA		845,182	2,036,758	5,257,106	9,663,000	19,111,000
- tax on income		37,721	34,806	38,000	42,500	4,124,120
+/- other		0,9	1,9	2,9	3,9	4,9
NOCFAT		807,462	2,001,954	5,219,109	9,620,504	14,986,885
		0	0	0	0	0
+/- Change Working Capital		-2,721,667	-978,476	61,499	2,323,081	2,409,995
- Capital Expenditure		0	0	0	0	0
Free Operating Cash Flow		-1,914,205	1,023,478	5,280,608	11,943,585	17,396,880
		0	1	0,87	0,76	0,66
		0	1,023,478	4,591,833	9,031,066	11,438,731
Discount rate	*15,0 %*				Terminal value	91,509,849
Long term growth rate	*2,5 %*				Enterprise Value	117,594,958
					- net financial debt	0
WACC	10,6 %					
Incremental Return on Equity	5,6 %				- Value of minority participations	0
					Value of the companies equity (mil)	118
Discount rate		13,0 %	14,0 %	15,0 %	17,5 %	20,0 %
Value of the equity		142	129	118	96	81
Value per share (CHF)		8,45	7,66	7,00	5,74	4,84

Source: Company Data, Silvia Quandt Research GmbH

Conclusion

OpenLimit is one of the best positioned companies to play the current and future trend of qualified digital signatures and eID cards. Providing a software capable of signing any document on any platform, we believe that OpenLimit is technologically well ahead of the competition with probably only Belgium's Certipost coming close.

We believe that similar to digitalisation this will become a huge market in the next few years and that now is the time to position oneself.

Our DCF Model comes to a valuation of € 7.00 from which we are taking a 40% discount for the micro-cap status and low stock-turnover of the company. This still gives us a value of €4.20 or a current upside potential of over 170%.

We initiate Open Limit with a Buy Rating and a price target of €4.20.

This analysis was prepared by Jacques Abramowicz, Head of Technology, Media and Telecommunications, and was first published on 16 September 2009. Silvia Quandt Research GmbH, Grüneburgweg 18, 60322 Frankfurt is responsible for its preparation.
German Regulatory Authority: Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Str. 108, 53117 Bonn and Lurgiallee 12, 60439 Frankfurt.

Publication according to article 5 (4) no. 3 of the German Regulation concerning the analysis of financial instruments (Finanzanalyseverordnung):

Number of recommendations from Silvia Quandt Research GmbH in 2009	Thereof recommendations for issuers to which investment banking services were provided during the preceding twelve months
31 buys	8
5 neutral	1
4 avoids	0

Company disclosures
Article 34b of the German Securities Trading Act (Wertpapierhandelsgesetz) in combination with the German regulation concerning the analysis of financial instruments (Finanzanalyseverordnung) requires an enterprise preparing a securities analysis to point out possible conflicts of interest with respect to the company or companies that are the subject of the analysis. A conflict of interest is presumed to exist, in particular, if an enterprise preparing a securities analysis:

(a) holds more than **5% of the share capital** of the company or companies analysed;
(b) has **lead managed or co-lead managed** a public offering of the securities of the company or companies in the previous 12 months;
(c) has provided **investment banking services** to the company or companies analysed during during the last 12 months for which a compensation has been or will be paid;
(d) is serving as a liquidity provider for the company's securities by issuing buy and sell orders;
(e) is party to an agreement with the company or companies that is the subject of the analysis relating to the preparation of the recommendation;
(f) or the analyst covering the issue has **other significant financial interests** with respect to the company or companies that are the subject of the analysis, for example holding a seat on the company's boards.

In this respective analysis the following of the above-mentioned conflicts of interests exist: e

Silvia Quandt Research GmbH, Silvia Quandt & Cie. AG, and its affiliated companies regularly hold shares of the analysed company or companies in their trading portfolios. The views expressed in this analysis reflect the personal views of the analyst about the subject securities or issuers. No part of the analyst's compensation was, is or will be directly or indirectly tied to the specific recommendations or views expressed in this analysis. It has not been determined in advance whether and at what intervals this report will be updated.

Equity Recommendation Definitions

Silvia Quandt Research GmbH analysts rate the shares of the companies they cover on an absolute basis using a 6 - 12-month target price. ‚Buys' assume an upside of more than 20 % from the current price during the following 6 - 12-months. These securities are expected to out-perform their respective sector indices. Securities with an expected under-performance to their respective sector index are rated ‚avoids'. Securities where the current share price is within a 5 % range of the sector performance are rated ‚neutral'. Securities prices used in this report are closing prices of the day before publication unless a different date is stated. With regard to unlisted securities median market prices are used based on various important broker sources (OTC-Market).

Disclaimer

This publication has been prepared and published by Silvia Quandt Research GmbH, a subsidiary of Silvia Quandt & Cie. AG. This publication is intended solely for distribution to professional and business customers of Silvia Quandt & Cie. AG. It is not intended to be distributed to private investors or private customers. Any information in this report is based on data obtained from publicly available information and sources considered to be reliable, but no representations or guarantees are made by Silvia Quandt Research GmbH with regard to the accuracy or completeness of the data or information contained in this report. The opinions and estimates contained herein constitute our best judgement at this date and time, and are subject to change without notice. Prior to this publication, the analysis has not been communicated to the analysed companies and changed subsequently. This report is for information purposes only; it is not intended to be and should not be construed as a recommendation, offer or solicitation to acquire, or dispose of, any of the securities mentioned in this report. In compliance with statutory and regulatory provisions, Silvia Quandt & Cie. AG and Silvia Quandt Research GmbH have set up effective organisational and administrative arrangements to prevent and avoid possible conflicts of interests in preparing and transmitting analyses. These include, in particular, inhouse
information barriers (Chinese walls). These information barriers apply to any information which is not publicly available and to which any of Silvia Quandt & Cie. AG and Silvia Quandt Research GmbH or its affiliates may have access from a business relationship with the issuer. For statutory or contractual reasons, this information may not be used in an analysis of the securities and is therefore not included in this report. Silvia Quandt & Cie. AG and Silvia Quandt Research GmbH, its affiliates and/or clients may conduct or may have conducted transactions for their own account or for the account of other parties with respect to the securities mentioned in this report or related investments before the recipient has received this report. Silvia Quandt & Cie. AG and Silvia Quandt Research GmbH or its affiliates, its executives, managers and employees may hold shares or positions, possibly even short sale positions, in securities mentioned in this report or in related investments. Silvia Quandt & Cie. AG in particular may provide banking or other advisory services to interested parties. Neither Silvia Quandt Research GmbH, Silvia Quandt & Cie. AG or its affiliates nor any of its officers, shareholders or employees accept any liability for any direct or consequential loss arising from any use of this publication or its contents. Any investments referred to herein may involve significant risk, are not necessarily available in all jurisdictions, may be illiquid and may not be suitable for all investors. The value of, or income from, any investments referred to herein may fluctuate and/or be affected by changes in exchange rates. Past performance is not indicative of future results. Investors should make their own investment decisions without relying on this publication. Only investors with sufficient knowledge and experience in financial matters to evaluate the merits and risks should consider an investment in any issuer or market discussed herein and other persons should not take any action on the basis of this publication.

Specific notices of possible conflicts of interest with respect to issuers or securities forming the subject of this report according to US or English law: None

This publication is issued in the United Kingdom only to persons described in Articles 19, 47 and 49 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2001 and is not intended to be distributed, directly or indirectly, to any other class of persons (including private investors). Neither this publication nor any copy of it may be taken or transmitted into the United States of America or distributed, directly or indirectly, in the United States of America.

Frankfurt am Main, 16 September 2009

Silvia Quandt Research GmbH . Grüneburgweg 18 . 60322 Frankfurt am Main . Germany . Tel: + 49 69 95 92 90 93 - 0 . Fax: + 49 69 95 92 90 93 - 11

RESEARCH

SILVIA QUANDT
RESEARCH GMBH

Silvia Quandt Research GmbH

Grüneburgweg 18
60322 Frankfurt, Germany
Fon: +49 (69) 95 92 90 93-0
Fax: +49 (69) 95 92 90 93-11
info@silviaquandt.de

16 September 2009