SILVIA QUANDT
RESEARCH GMBH

RESEARCH

OPENLIMIT HOLDING AG – REAPING THE REWARDS OF CONTINUED COMMITMENT

_GERMAN eID TO BE INTRODUCED THIS NOVEMBER. OPENLIMIT WILL SUPPLY THE CITIZEN CLIENT

_SECDOCS SUBMITTED FOR CERTIFICATION BY THE BSI

_DIBAS PROJECT AWARDED BY FUJITSU TECHNOLOGY SOLUTIONS, LARGEST MAIL-IN BOX PROJECT FOR OPENLIMIT TO DATE

_BUY RECOMMENDATION, FAIR VALUE € 3.02 (4.20)

Jacques Abramowicz, Head of Technology, Media and Telecommunications
25 May 2010

OpenLimit Holding 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 (m)
€ 27.49
(note: market cap in € not CHF)

No. of outstanding shares (m)
18.087 m common

Daily traded volume

Indices
General Standard

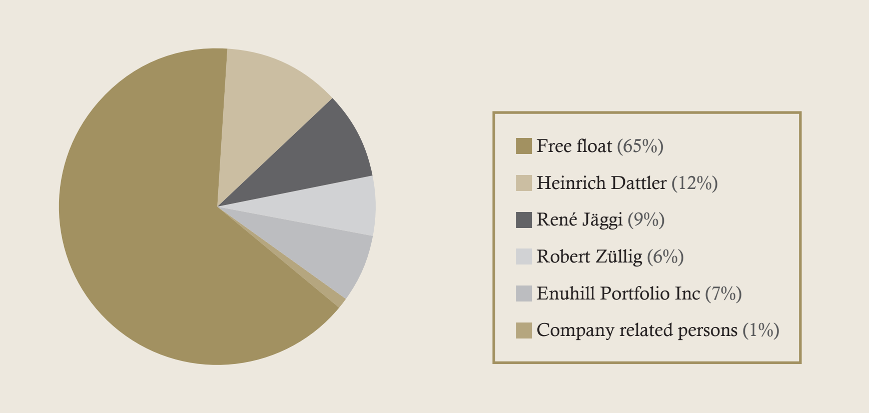
Next Event
31 May 2010 AGM

Free Float
65%

CHF m	*2009*	*2010e*	*2011e*	*2012e*	*2013e*
Revenues	6.587.862	8.234.828	10.293.534	13.896.271	19.454.780
Total Income	9.560.344	12.009.880	15.012.350	19.322.909	22.168.099
EBITDA	747.349	2.610.845	4.072.487	6.841.543	9.035.808
EBIT	-1.230.482	119.311	958.069	3.259.962	7.245.017
Profit	-804.181	336.936	1.084.569	3.167.162	5.967.564
EPS	-0.05	0.02	0.06	0.18	0.33
Employees	46	53	62	70	76

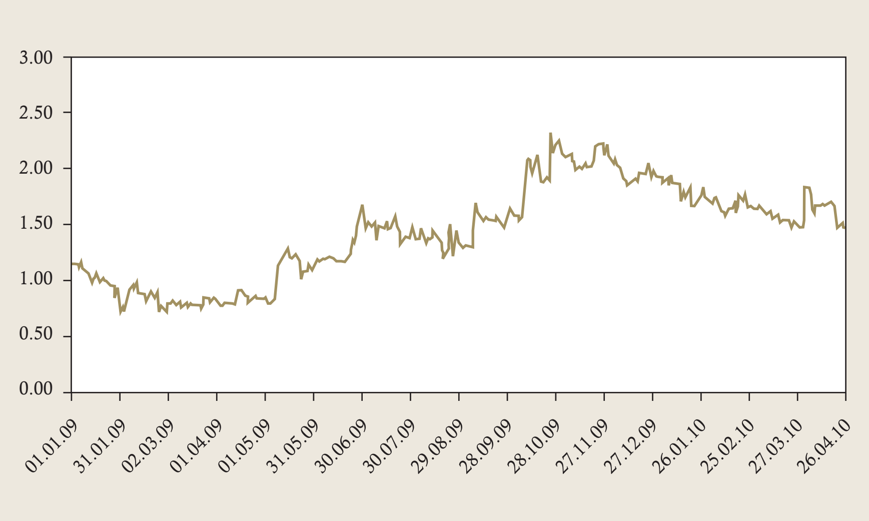
Source: Company data, Silvia Quandt Research GmbH

Shareholder Structure



Source: Silvia Quandt Research GmbH, Company Data

Company Share Price Development



Source: Silvia Quandt Research GmbH, Bloomberg, Prices as of 11.05.2010

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 will 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. It currently holds the only certified EAL 4+ solution.

We believe that the approval of the German Bundestag on December 18th 2008, to introduce an electronic identity card in November 2010 and the award of the project on November 4th 2009 to a Siemens AG led consortium will be the big breakthrough that this industry has been waiting for and will show why the faith placed in OpenLimit was well founded.

We see enormous potential in OpenLimit's Digital Signature & MigSafe products, 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 Holding AG

About OpenLimit Holding 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 qualified electronic signature can be generated in online forms using the OpenLimit signature software. This is legally accorded the same status as the hand-written 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 such solution worldwide 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 OpenLimit technologies for electronic archives supplement archiving solutions taking into consideration legally compliant and audit-secure, long-term archives.

As well as implementation, consulting and training services, OpenLimit offers all-round, 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.

Recent Highlights

__**Nov 4th, 2009**
awarded Bürger Client by Siemens AG

__**Feb 8th, 2010**
awarded large contract for the DiBas Project of German Federal Employment Agency by Fujitsu Technology Solutions

__**March 5th 2010**
BSI certification ID for SecDocs commenced

__**April 8th 2010**
Fujitsu & OpenLimit prepare SecDocs for global operation

DiBAS is one of largest and most ambitious public sector projects in Europe. In order to reduce the amount of paper used by the administration, all documents of the Federal Employment Agency will be digitized, signed and electronically stored in order to make documents available in electronic form in the future. In addition to existing documents, new documents will also be maintained electronically.

The project volume is comprised of a fixed component for the software licenses implemented, services, software maintenance per annum and a variable component per signature to be applied to the estimated one to three billion documents. Based on these parameters, the project volume over the next five years will be in the seven digit EUR range. The parties agreed on confidentiality pertaining to exact contract conditions.

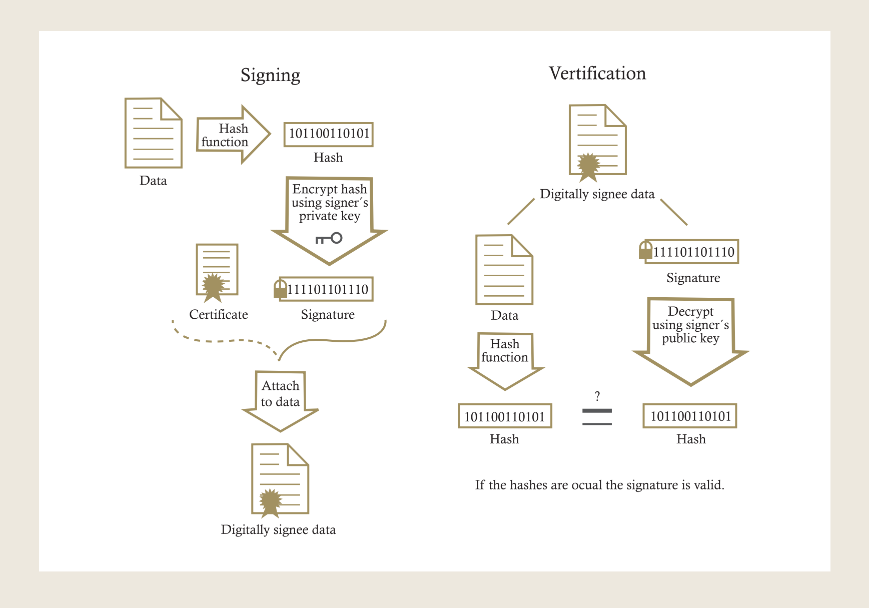
Digital Signature Market

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.

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 in 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 terms of what OpenLimit does, we are talking of a qualified digital signature based on an EAL 4+ standard the currently most sophisticated and secure encryption out in the market.



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 attach 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.

Citizen Client

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

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 were needed. This is probably why the consortium led by Siemens AG and involving both the Bundesdruckerei and OpenLimit Signcubes AG won the pitch.

Sales by Products

All of OpenLimit's product lines have in common that they are based on secure digital signage of documents or document containers. With its expertise in EAL4+ OpenLimit is ideally placed to benefit from the trends of expanding digital signatures into new fields and markets. OpenLimit has three main product lines:

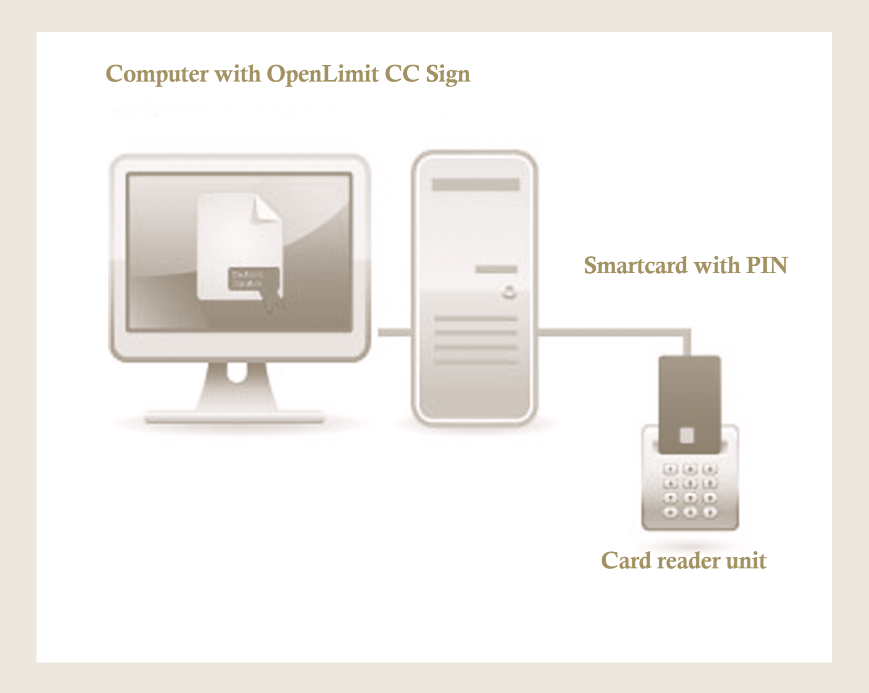
1. Security Technologies

a) Client
b) Integration and Server
c) Products for Form Server

2. Document Technologies

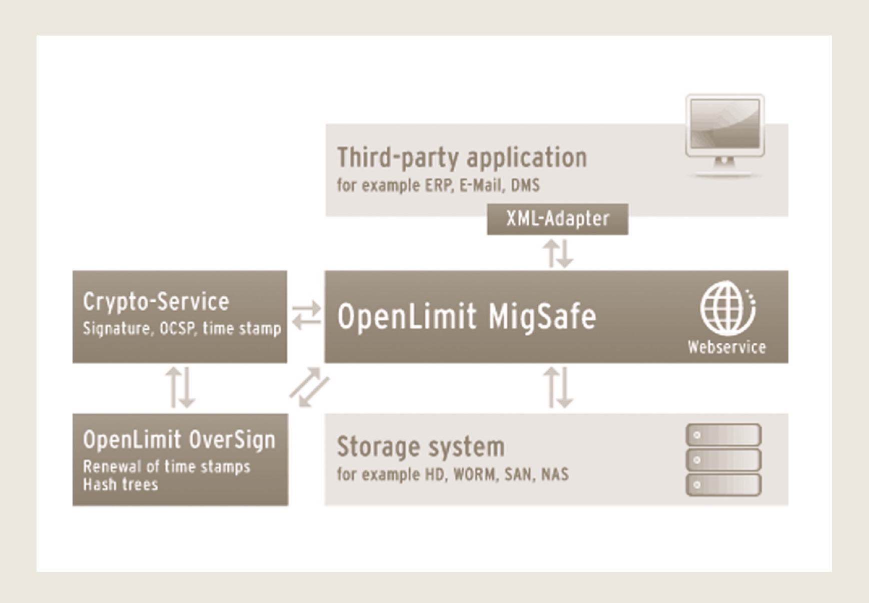
3. Technologies for eArchives

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.

__Only certified EAL 4+ product portfolio.

Weaknesses

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

__Slow in getting its standard implemented by organisations such as Sparkassenverlag and VR-Gruppe.

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 can turn out to be the biggest opportunity of them all as legal requirements for archiving get longer. Here, a secure manipulative-free electronic solution can lead to huge cost savings for companies.

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 although we don’t believe that there will be only a single standard across Europe.

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 hand-written 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 hand-written 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 is intended to be 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. Note that the eAuthorisation is automatic and free whereas the qualified digital signature would have to be purchased separately.

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

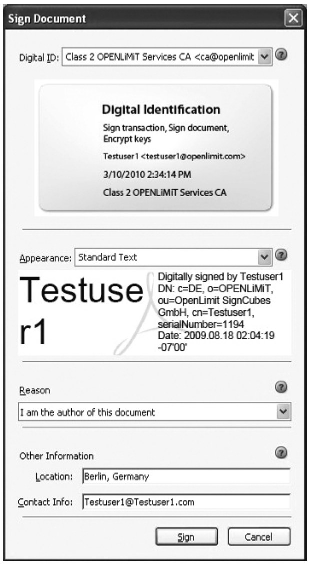
This area is covered by OpenLimit's CC-Sign

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).



Sign Document

Digital ID: Class 2 OPENLiMiT Services CA <ca@openlimit

Digital Identification

Sign transaction, Sign document, Encrypt keys

Testuser1 <testuser1@openlimit.com>

3/10/2010 2:34:14 PM

Class 2 OPENLiMiT Services CA

Appearance: Standard Text

Testuser1

Digitally signed by Testuser1
DN: c=DE, o=OPENLiMiT, ou=OpenLimit SignCubes GmbH, cn=Testuser1, serialNumber=1194
Date: 2009.08.18 02:04:19 -07'00'

Reason: I am the author of this document

Other Information

Location: Berlin, Germany

Contact Info: Testuser1@Testuser1.com

Source: OpenLimit AG

Financials

Income Statement

CHF	*2009*	*2010e*	*2011e*	*2012e*	*2013e*
Revenue	6.587.862	8.234.828	10.293.534	13.896.271	19.454.780
add S/W development	2.972.482	3.775.052	4.718.815	5.426.637	2.713.319
Total Income	**9.560.344**	**12.009.880**	**15.012.350**	**19.322.909**	**22.168.099**
Cost of goods sold	135.213	186.153	315.259	483.073	554.202
Personel expenses	6.653.574	6.986.253	7.824.603	8.998.293	10.078.089
Depreciation	1.977.831	2.491.534	3.114.418	3.581.581	1.790.790
Operational expenses	2.024.208	2.226.629	2.800.000	3.000.000	2.500.000
Income from Operations	**-1.230.482**	**119.311**	**958.069**	**3.259.962**	**7.245.017**
Financial Income	17.253	22.500	1.500	2.200	45.000
Financial expense	171.467	224.875	250.000	275.000	12.500
Income before Taxes	**-1.384.695**	**-83.064**	**709.569**	**2.987.162**	**7.277.517**
Taxes	-580.514	-420.000	-375.000	-180.000	1.309.953
Net Income	**-804.181**	**336.936**	**1.084.569**	**3.167.162**	**5.967.564**
Dividend paid	0	0	0	2.000.000	3.000.000
Net income after dividends	**-804.181**	**336.936**	**1.084.569**	**1.167.162**	**2.967.564**
Shares outstanding	17.586.885	18.086.885	18.086.885	18.086.885	18.086.885
DPS	0.00	0.00	0.00	0.11	0.17
EPS	-0.05	0.02	0.06	0.18	0.33

Source: Company data, Silvia Quandt Research GmbH

Balance sheet

CHF	*2009*	*2010e*	*2011e*	*2012e*	*2013e*
Receivables	7.305.910	6.707.191	8.855.650	10.407.315	11.394.311
Cash and equivalents	1.357.773	422.500	600.500	1.850.000	3.550.000
Current Assets	**8.663.683**	**7.129.691**	**9.456.150**	**12.257.315**	**14.944.311**
Intangible Asset	4.682.915	5.966.433	7.570.830	9.415.887	10.338.415
Plant & Equipment	144.769	150.000	155.000	185.000	198.000
Non-current Assets	**4.827.684**	**6.116.433**	**7.725.830**	**9.600.887**	**10.536.415**
Total Assets	**13.491.368**	**13.246.124**	**17.181.980**	**21.858.202**	**25.480.726**
Share capital	5.276.066	5.276.066	5.276.066	5.276.066	5.276.066
Share premium	11.063.645	11.063.645	11.063.645	11.063.645	11.063.645
Provisions for Bonuses	1.412.716	1.624.623	1.868.317	2.148.564	2.470.849
Accumulated profit (loss)	-5.032.553	-5.836.735	-5.499.799	-4.415.230	-3.248.068
Equity	**12.719.874**	**12.127.599**	**12.708.229**	**14.073.045**	**15.562.492**
Accounts payable	492.484	758.354	3.698.008	6.654.604	7.708.234
Tax liabilities	18.784	0	325.743	585.552	1.535.000
Current liabilities	**511.268**	**758.354**	**4.023.751**	**7.240.156**	**9.243.234**
Pension liabilities	260.226	360.170	450.000	545.000	675.000
Total equity & liabilities	**13.491.368**	**13.246.123**	**17.181.980**	**21.858.201**	**25.480.726**

Source: Company data, Silvia Quandt Research GmbH

Cash flow

CHF	*2009*	*2010e*	*2011e*	*2012e*	*2013e*
Net Income	-804.182	336.936	1.084.569	3.167.162	5.967.564
Tax	46.486	60.648	195.222	570.089	1.074.162
Financial Income/expense	23.161	-12.500	-17.250	-20.154	21.346
Depreciation	1.977.831	2.491.534	3.114.418	3.581.581	1.790.790
Loss of receiables	8.000	25.000	22.000	27.500	26.500
Loss on sale of equipment	406	0	0	0	0
Exchange differences	-23.345	-25.000	-25.000	-25.000	-25.000
Share based payments	1.412.716	1.624.623	1.868.317	2.148.564	2.470.849
Increase (decrease) in receivables	-1.869.660	598.719	-2.148.459	-1.551.665	-986.996
Increase (decrease) in other liabilities	-129.577	-265.870	-2.939.654	-2.956.596	-1.053.630
Net Cash from Operating activities	**641.836**	**4.834.091**	**1.154.164**	**4.941.481**	**9.285.585**
Interest received	17.253	22.500	1.500	2.200	45.000
Interest paid	-40.414	-35.000	-18.750	-22.354	-23.654
Taxes paid	-32.527	-65.000	-195.000	-620.000	-850.000
Net Cash after Interest & Taxes	**586.148**	**4.756.591**	**941.914**	**4.301.327**	**8.456.931**
Investments in intangible assets and equipment	-3.066.080	-1.283.518	-1.604.397	-1.845.057	-922.528
Net Cash from Investmentactivities	**-3.066.080**	**-1.283.518**	**-1.604.397**	**-1.845.057**	**-922.528**
Capital increase	548.842	150.000	0	0	0
Surplus capital	3.187.428	794.953	0	0	0
Cash flow from Financing actvites	**3.736.270**	**0**	**0**	**0**	**0**
Net Increase in Cash & cash equivalents	**1.256.338**	**3.473.073**	**-662.484**	**2.456.271**	**7.534.403**
Cash & cash equivalents beginning of year	101.435	1.357.773	4.830.846	4.168.362	6.624.633
Cash & cash equivalents end of year	1.357.773	4.830.846	4.168.362	6.624.633	14.159.036

Source: Company data, Silvia Quandt Research GmbH

Please note that since it is impossible to predict when Options are exercised, we have not accounted for those going forward past Q1 2010.

Discounted cash flow

		2009	*2010e*	*2011e*	*2012e*	*2013e*
Sales		6.587.862	8.234.828	10.293.534	13.896.271	19.454.780
EBITDA		747.349	2.610.845	4.072.487	6.841.543	9.035.808
- tax on income		-580.514	-420.000	-375.000	-180.000	1.309.953
NOCFAT		1.327.863	3.030.845	4.447.487	7.021.543	7.725.854
		0	0	0	0	0
+/- Change Working Capital		641.836	4.834.091	1.154.164	4.941.481	9.285.585
- Capital Expenditure		-3.066.080	-1.283.518	-1.604.397	-1.845.057	-922.528
Free Operating Cash Flow		-1.096.381	6.581.418	3.997.254	10.117.967	16.088.911
		0	1	0.87	0.76	0.66
		0	6.581.418	3.475.873	7.650.637	10.578.720
Discount rate	15.0%	Terminal value				84.629.762
Long term growth rate	2.5%	Enterprise Value (CHF mil) - net financial debt				112.916.410 0
WACC	10.6%					
Incremental Return on Equity	5.6%	- Value of minority participations				0
		Value of the companies equity (€ mil)				78

Discount rate	13.0%	14.0%	15.0%	17.5%	20.0%
Value of the equity	93	85	78	64	55
Value per share (Euro)	5.16	4.70	4.31	3.56	3.03

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 similarly to digitalisation this will become a huge market in the next few years and that now is the time to position one-self.

Our DCF Model comes to a valuation of € 4.31 from which we are taking a 30% discount for the micro-cap status and low stock-turnover of the company. This still gives us a value of € 3.02 or, a current upside potential of nearly 100%.

We remain a Buy on OpenLimit with a price target of € 3.02 (4.20)

This analysis was prepared by Jacques Abramowicz, Head of Technology, Media and Telecommunications and was first published 25 May 2010. 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 2010		Thereof recommendations for issuers to which investment banking services were provided during the preceding twelve months
Buy	49	29
Neutral	20	3
Avoid	7	1
Under Review	1	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** for the company or companies analysed 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 production 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 this 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: c

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. Copyright and database rights protection exists in this publication and it may not be reproduced, distributed or published by any person for any purpose without the prior express consent of Silvia Quandt Research GmbH. All rights reserved. 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, 25 May 2010

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

25 May 2010