

ISABEL AND SARBANES-OXLEY

1. INTRODUCTION.....	1
2. BELGIAN-BASED COMPANY, ISABEL NV/S.A., AND ITS COMPLIANCE WITH BELGIAN & EUROPEAN REGULATIONS.....	2
3. "ISABEL DUE CARE"	3
4. ISABEL SOFTWARE IN MORE DETAIL.....	4
5. RESPONSIBILITY OF THE ISABEL USER.....	8
6. IN A NUTSHELL: SECURITY ADVICE FOR SOX	10
7. FURTHER INFORMATION	10

1. INTRODUCTION

The Sarbanes-Oxley Act (abbreviated to SOX) was passed in June 2002 as a consequence of financial scandals. SOX is based on a bill tabled by Senator Paul Sarbanes and Congressman Michael Oxley and applies to companies listed on the New York Stock Exchange (or more precisely: companies registered with the U.S. Federal Stock Exchange Commission). Mainly, the Act directly affects American companies. Only about 500 non-US companies are listed in New York (these include four Belgian companies). The Act is, of course, also important for foreign subsidiaries of American multinationals. Recently, Deloitte estimated the number of these subsidiaries in Belgium at about 300. Foreign companies that are also listed on the NYSE were required to comply with SOX regulations from 15th July 2005. However, on 2nd March 2005, the US Securities and Exchange Commission (SEC) extended this deadline by one year to 15th July 2006. The fiscal year of many companies runs in parallel with the calendar year. Consequently, they will need to be SOX-compliant by 31st December 2006, including testing their control regulations for effectiveness.

The Sarbanes-Oxley Act is made up of 69 sections, dealing mainly with financial control, the quality of accountancy records and procedures, independence of auditors, etc.

However, the provision quoted most often is Section 404, which states that it is the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. As a consequence of this provision, there has been an urgent requirement for technical and organisational means for controlling the internal processes within companies in a more systematic manner. This explains the need for "SOX compliance" in many companies for their financial reporting tools. For some subsidiaries of American multinationals, Isabel software is one of the software packages used for conducting financial transactions.

Companies subject to SOX have to get proof of due diligence from their suppliers. This can be done through a SAS 70 certificate (www.sas70.com).

2. BELGIAN-BASED COMPANY, ISABEL NV/S.A., AND ITS COMPLIANCE WITH BELGIAN & EUROPEAN REGULATIONS

Isabel NV/S.A. is a Belgian company and as such is governed by Belgian and European legislation.

In Europe, the general topic of “corporate governance” has been taken up and transposed into a number of non-binding codes and guidelines. The Basel II Accord in the financial sector and the Belgian “Code Lippens” are illustrative examples of this development. Ultimately, the need for compliance with Sarbanes-Oxley has led to an upsurge in awareness regarding ICT security.

The discussion about Sarbanes-Oxley and the Corporate Governance Codes should not be allowed to shunt the European legislation that already exists in the area of security into the background. Back in 1995, in its general Data Protection Directive, Europe introduced a provision that specifically requires every company involved in the processing of personal data (data about private individuals, such as names, addresses, financial data, etc.) to implement security for protecting such information.

Following this provision, the controllers and processors of personal data had to take “adequate” security measures. “Adequacy” in this context is measured against four criteria: 1) the measure taken has to be “state-of-the-art”, 2) the specific nature of the data has to be taken into account (i.e. stricter measures for financial and health data, etc., compared with data containing just contact details), 3) measures should be in line with the potential risks, and 4) investments in security must be proportionate to the potential of the controller or the processor (i.e. stricter requirements for large commercial organisations than for SMEs). As far as Isabel is concerned, these security measures are explained in the following paragraph.

The presence of specific legislation relating to security and risk management should not allow us to forget that every person and every company has a general duty of care. If the lack of appropriate security measures leads to harm being caused to third parties, the liability will automatically be incurred of any company neglecting to apply best practices in this field and to behave “responsibly”. On the other hand, and contrary to the specific statutory security obligations described above, general liability can, at least to a certain extent, be reduced by so-called disclaimers.

3. “ISABEL DUE CARE”

Isabel is not subject to SOX nor does it have a SAS 70 audit report to supply to its customers which are subject to SOX. As the main supplier of banking software and Isabel services, Isabel is governed by Belgian banking regulations. Therefore Isabel complies with the regulations pertaining to the syndicated auditing of the banks. For more information, go to: http://www.cbfa.be/nl/ki/circ/pdf/d1_97_4.pdf

Isabel also has a TruSecure certification. See: <http://www.isabel.be/contrib/documents/en/trusecure.certif.letter.pdf> TruSecure Certification is your assurance that an organisation has widely-recognised and accepted measures in place to secure its environment and can confidently conduct business in a world of ever-changing risk. TruSecure Corporation (recently merged with Betrusted into Cybertrust - www.cybertrust.com) is a worldwide leader in managed security and assurance solutions for organisations connected to the Internet. More than just a seal of approval, TruSecure-certified status demonstrates to customers, partners and vendors that an organisation has implemented due diligence and made security a priority in order to safeguard its critical information and assets. The TruSecure Certified Seal indicates that the certified organisation employs widely-recognised security processes and technologies in order to maintain a proactive and comprehensive information security programme. TruSecure Certified customers have had their security controls, procedures and policies examined, measured and validated by the TruSecure Corporation team of security experts.

4. ISABEL SOFTWARE IN MORE DETAIL

Isabel was created by a consortium of Belgian banks to provide an integrated business-to-business eBanking solution. Isabel has a secure network that is used to support the exchange of financial and banking information, electronic mail, information retrieval and eGovernment transactions. Supporting this infrastructure, Isabel acts as its own Certification Authority. It also provides the necessary security and communication software required to integrate with other services. Within its own Public Key Infrastructure, Isabel maintains user certificates, a Certification Authority and issues users with smart cards that contain their private keys.

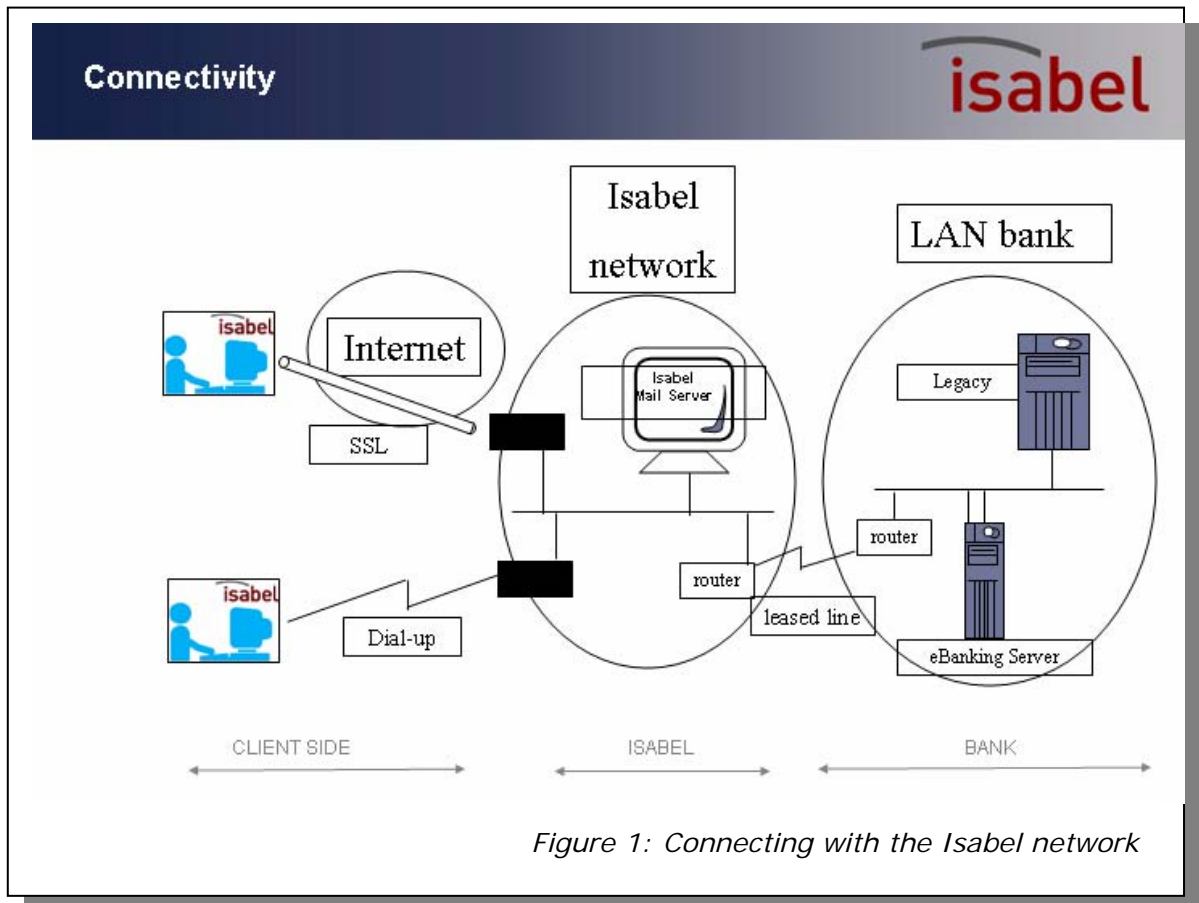
Isabel uses the RSA public key cryptosystem. The user's public key is made accessible publicly, while the private key remains secret and stays in the possession of the owner. Although the keys are mathematically related, there is no way of computing them externally. Using RSA for confidentiality is performed with the public key of the receiver, while decryption is carried out with the receiver's private key. Isabel has its own PKI and consequently stands at the top of its own trust hierarchy.

The public key enables the Isabel customer to check the digital signature attached using the matching private key. Information can also be encoded and decoded using the key pair in order to ensure its confidentiality. If this is the case, only the private key is able to decode information encoded with the matching public key.

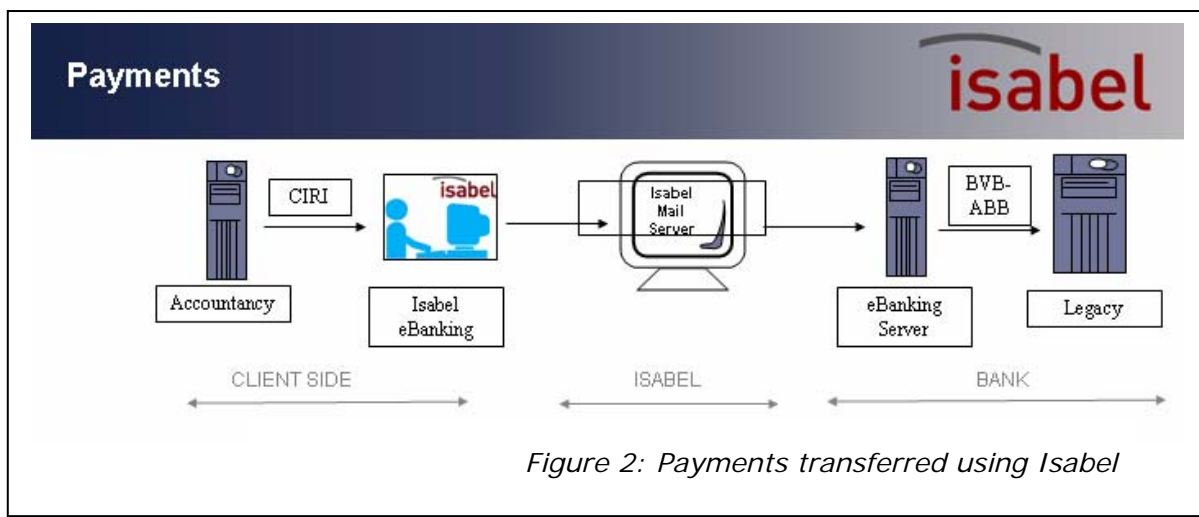
A digital signature provides the guarantee that the purported sender actually sent a particular message. Digital signatures therefore authenticate the sender of a message and guarantee the message's integrity. The assurance that the sender cannot deny the sending of the message is also granted, preventing the sender from escaping any obligations entered into by attaching the digital signature.

Isabel operates as a mailbox, a secure intermediary and conduit of confidential information. For example, payments can be prepared manually in the Isabel program, or else they can be imported into the Isabel software from an accountancy or ERP package.

The workflows and operation of the Isabel system can best be seen through a series of diagrams:



There are two ways in which client authentication can be performed on the Isabel network. The first is associated with a dial-up connection with an Isabel Point of Presence Server, and is achieved through verification of the client's signature. The second process is associated with Internet access to the Isabel network using mutual authenticated SSL protocol. In this case, verification of an Internet user's signature is performed by an SSL server proxy.



Customers can import payment files from their accountancy system or create payment orders from Isabel Business Suite 5.0.

- Important: When payment files are imported from an accountancy or ERP package, verification between the accountancy or ERP package and the Isabel Business Suite can be carried out.

To ensure the integrity of payment files imported from an accountancy or ERP package into Isabel, hash values can be calculated for these payment files before they are exported from the accountancy or ERP package. These hash values can be verified in the Isabel software. Some accountancy and ERP Package provide this possibility, others will provide it in the future.

The SHA-1 (http://www.w3.org/PICS/DSig/SHA1_1_0.html)

digest algorithm should be used for generating the digest. Afterwards the hash of the payment file imported into Isabel can easily be compared with the original hash value.

In Isabel Business Suite, customers sign their payment orders digitally and send them to Isabel.

Important: The person who signs the payment should verify the payment he or she is signing with care. Preferably, 2 or 3 persons should be involved in the signing process in order to avoid any possible fraud.

Once the payment has been signed with the Isabel signature, there is no further risk involved (i.e. authenticity, integrity and non-repudiation are guaranteed).

The Isabel mail server will send the instructions to the bank's central mailbox.

eBanking server de-encapsulates the payment file and checks the customer's signature(s).

The bank legacy receives the payments files from the eBanking Server.

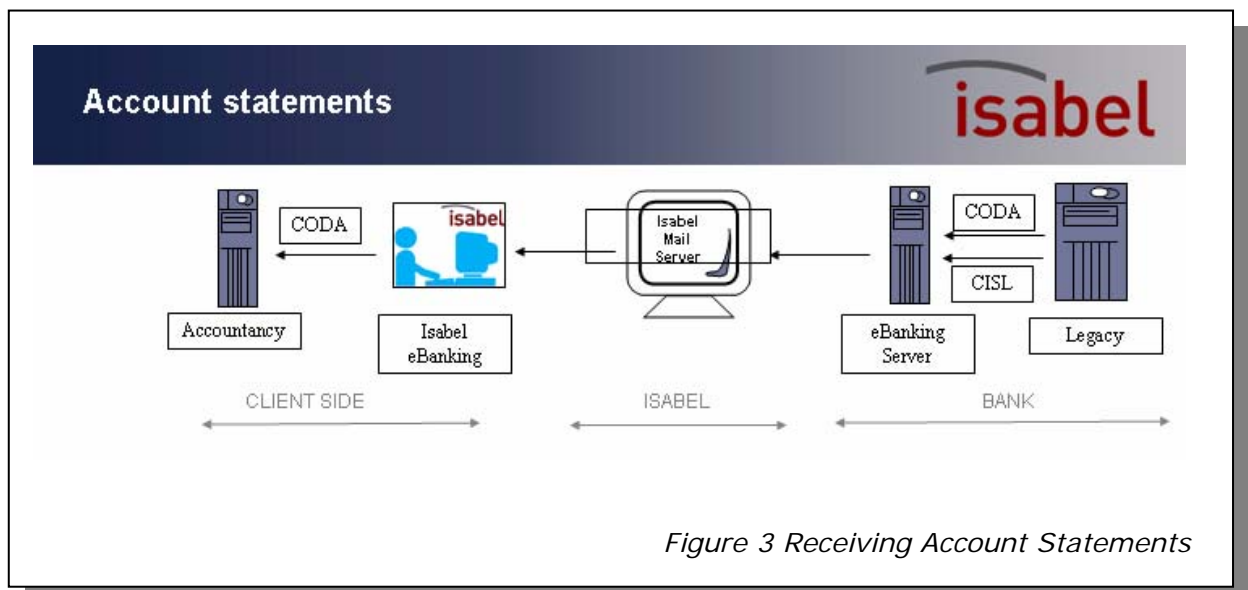


Figure 3 Receiving Account Statements

The bank legacy generates CISL + CODA* files and sends them to the eBanking Server.

The eBanking Server encapsulates the files, signs and sends them to Isabel.

The Isabel mail server deposits the messages to the customers' central mailboxes.

When connecting to Isabel, customers replicate the statements into their local Isabel Business Suite mailbox. Isabel Business Suite de-encapsulates CISL/CODA and checks the bank signature.

Customers can export the account statements to their accountancy systems in CODA format.

Isabel cannot change information without being noticed by the customer or the bank, guaranteed by the digital signature. Isabel only acts as a message transfer system.

* More information on the Belgian Banking Standards can be found on http://www.abb-bvb.be/gen/en/profession_systeme.html

5. RESPONSIBILITY OF THE ISABEL USER

No matter how secure and sophisticated Isabel security may be, caution is still recommended. The following should retain the attention of the SOX compliance officer and appropriate internal policies at the customer side should exist.

1. Isabel takes every possible step to guarantee the security of its network. You hold one aspect of this security **in your own hands**: the Isabel Secure Signing Card. The Isabel Secure Signing Card contains a chip that is much more difficult to copy than the conventional magnetic strip. This gold-coloured rectangle computes the personal signature that gives you access to the Isabel network. We therefore recommend that our users, if they are not already doing so, use the Secure Signing Card (1024 bits) and stop using the older type of Smart Card (512 bits). The Isabel Secure Signing Card provides the highest level of security.
2. This means it is vitally important that the Secure Signing Card does not fall into anyone else's hands. You must also **keep your password absolutely secret**. So, what happens if someone tries to log in using your Secure Signing Card and does not know the password? The card will be rendered unusable after five failed attempts. One thing is certain: **if your Secure Signing Card is lost or stolen**, you must place a block on the card immediately.
3. The Secure Signing Card can be used in 2 ways:
 - a. signature for payment authorisation: the card is personal and should NOT be transferred.
 - b. signature for transfer only (technical signature i.e. it has no payment authorisation power). In some companies, a single Secure Signing Card may be used by more than one person. In such a case, you should specify explicitly who has access to where the Secure Signing Card is kept and who knows the password. In case of change to the user group of a shared Secure Signing Card, the password should also be changed.

4. Isabel has also incorporated extremely sophisticated and effective systems that are designed to protect the electronic transactions of Isabel users. Of course, Isabel is unable to offer any cast-iron guarantees against any breaches of computer protocol that occur in the customer's workplace, such as the incorrect or unauthorised use of PCs, software and hardware. This applies regardless of whether these breaches of protocol originate from the websites that our customers may visit, by way of the communication lines they use to send their messages, via their LAN network or for any other reason that is beyond Isabel's control. **Each and every user must be totally responsible for the use of his or her PC (up-to-date anti-virus software, anti-spyware program, firewalls, patches,...).**
5. Signatories of payments should preferably work on a different PC to the Isabel PC on which the payments are encoded. Signatories can sign individually or in conjunction with other signatories from different locations using the MultiSign module. Signatories should check the files they sign very carefully.
6. Signatories should compare hash values generated by the Isabel Business Suite with values provided by their accountancy or ERP package. This is the highest level of guarantee for the user to be sure that the payment files have not been tampered with.

6. IN A NUTSHELL: SECURITY ADVICE FOR SOX

- Use Isabel recommended “state-of-the-art technology” currently the Isabel Business Suite 5.0 software and a Secure Signing Card chip card (1024 bits).
- Implement internal controls for (Isabel) PC protection.
- Implement internal security controls for transfer of files between your accounting software and the Isabel application.
- Mitigate fraud risk by using multiple signatories who have to sign jointly.
- Mitigate fraud risk by keeping separate PCs for signatories and for encoding.
- Implement controls to make signatories aware that What You See Is What You Sign, and have them verify before they sign.
- Implement controls to make signatories aware that their Secure Signing Card is personal: the person to whom the Secure Signing Card and password belong can sign on behalf of the signatory (non-repudiation).
- Make your accounting package provide hash values which can be compared with the Isabel Business Suite hash values.

7. FURTHER INFORMATION

If you have further questions about Isabel and Sarbanes Oxley, please send an e-mail to Isabel’s Security Manager, Bart Moerman: bmoerman@isabel.be

For more general information on:

- **Isabel**: www.isabel.be
- Sarbanes-Oxley:
 - <http://www.aicpa.org/sarbanes/index.asp>
 - <http://www.law.uc.edu/CCL/SOact/toc.html>
- the **payment systems and banking standards in Belgium**: www.abb-bvb.be
- the Belgian Banking, Finance and Insurance Commission: www.cbfa.be
- SAS 70 Certificate (www.sas70.com)
- How to find the Isabel hash value? Go to www.isabel.be. Click on the icon **Isabel Web Support** and enter 51362 in the Search Screen.