



EDI and e-invoice Software-as-a-Service

White Paper
BABELGOM 2.0

October 2008

Contents

INTRODUCTION.....	2
EXECUTIVE SUMMARY.....	3
CHAPTER 1: FUNCTIONALITIES OVERVIEW.....	4
CHAPTER 2: QUALITY AND SECURITY MANAGEMENT.....	8
CHAPTER 3: USER SUPPORT.....	13

INTRODUCTION

The benefits to businesses of EDI in general and e-invoicing in particular have largely been documented in multiple reports. An EC report¹ quotes 238 billion Euros, 400,000 tons of paper, 2 700 tons of ink, 160 million liters of petrol as an estimate of what European businesses would save by adopting e-invoice. The benefits are much larger if one includes other traditional B2B document flows such as purchase orders and dispatch notes for example.

The 2 traditional EDI methods

The 2 traditional methods to automate data exchanges between business partners (EDI) are either (1) to acquire EDI translation software or (2) to join a B2B integration hub. The first method is also the historical method. Companies buy (or custom build) and install a B2B communication system within a company's internal IT environment and organize point-to-point communication with other companies via private networks (X400 network or, so called, value-added networks).

This way of doing EDI enables a great deal of flexibility. Participants control the individual B2B relationships and their technical components. However, this method requires important investment in money, time and skills. Larger companies have traditionally opted for this method.

Together with Internet, a second method to do EDI arose: the B2B integration hub. Point-to-point communication is replaced by a central hub such that one communication to the central hub is sufficient to reach all other partners. The B2B integration hub enables to rapidly deploy to a community of trading partners. The value proposition of the B2B integration hub is to create one technical link between an individual company and the hub. B2B data flows are then technically organized by the hub. This method corresponds to outsourcing to a Third-Party. It leads to a loss of control and sometimes a loss of speed when comes the time to connect to a new business partner. Medium-sized companies have usually chosen this method.

What's different about Babelgom?

Babelgom B2B integration Software-as-a-Service has bridged the 2 traditional methods. Babelgom enables customers to connect directly to their partners, avoiding the need for B2B intermediaries. Customers have therefore total **control** over their data flows. In addition, Babelgom doesn't require the acquisition of in-house software and infrastructure. Customers can avoid the investment and the operational costs of running an EDI infrastructure and benefit from automated data exchange at much **lower costs**. The community of Babelgom users can share common components of data flows (eg. the invoice format of Carrefour Belgium) through a catalogue of components such that the time it takes to build new channels decreases as the community increases.

Babelgom offers **absolute flexibility** to companies of all sizes and at any level of data exchange volumes. They can decide to control data flows or outsource some of it to external IT partners. They can quickly deploy to business partners or stage an on-boarding project based on general business priorities.

This document describes the innovative EDI and e-invoice Software-as-a-Service (SaaS) developed by Babelgom. It is addressed to people evaluating an EDI and e-invoice solution in detail. We also advise these people to register online now to freely discover for themselves what Babelgom can do and how it works.

¹ « European Electronic Invoicing final report produced » by the European Commission Informal task force on e-invoicing http://ec.europa.eu/information_society/eeurope/i2010/docs/studies/eei-3.2-e-invoicing_final_report.pdf.



EXECUTIVE SUMMARY

Babelgom B2B integration Software-as-a-Service allows organizations to automate cross-company processes and enables the secure exchange of structured and recurrent document such an order, an invoice, a payslip, a report, a payment advice, etc.

All it takes it to register online (www.babelgom.net) to be ready to automate data exchange with ANY business partner or computer applications. Babelgom guarantees full-proof security, unlimited scalability and first-class performance. Babelgom is the solution to rapidly connect to a trading community while retaining full control over data flows.

Babelgom offers a wide range of functionality to build and administer channels between 2 systems. Babelgom supports AS/2, FTP(s), sFTP, web, email and SOAP communication and supports XML, Excel, EDI, CSV and any custom flat file formats.

Babelgom is equipped with multiple functionalities such as drag&drop mapping interfaces, message validation, electronic signature, lookup tables, test environment, routing, email notifications, catalogue of ready-to-use components, message tracking, issue management, access and privilege management, capacity and performance management, storage management.

Babelgom software and infrastructure is managed using the strictest quality and security management processes. At the time of writing Babelgom was in the process of ISO27001 certification that provides the management system to ensure total security in highly technical environments. Babelgom is hosted in 2 redundant data centers. All systems are permanently monitored by internal and external systems. Storage is encrypted to guarantee confidentiality. Babelgom conforms to legal requirements in e-invoicing and provides customers with advanced certificates to enable them to transfer and archive invoices in a legally compliant way. The Babelgom solution has been audited and qualified as compliant to the relevant EU regulation by Professors Dumortier (KUL) and Quisquater (UCL), internationally recognized experts in the fields of electronic signature and cryptography.

Babelgom offers helpdesk support. In addition, Babelgom recommends the usage of the community forum where users can share experiences with other users. Babelgom develops partnerships with software vendors and IT integrators such that customers can find help from the most effective source whenever required.

Babelgom regularly organises training sessions and plans to develop a certification programme for qualified individuals.

CHAPTER 1: FUNCTIONALITIES OVERVIEW

Babelgom is the first B2B integration Software-as-a-Service. Babelgom provides EDI translation software and B2B communication gateways organized in a full service proposition. Babelgom services are fully available on-demand via a web-browser. There is no software or hardware to buy and maintain in-house and yet, Babelgom is under the full control of users.

This chapter briefly describes the main functionalities of the software

Building channels

A channel is the collection of components that must be assembled within Babelgom to organize an automatic data flow from an external system A to another external system B. The key components will be

- (1) the way Babelgom will be interfaced with system A, called the "gateway IN",
- (2) the way system A formats data, called the "message IN"
- (3) the format in which system B wants to receive data, called the "message OUT"
- (4) the way Babelgom will be interfaced with system B, called the "gateway OUT"

In building channels, Babelgom includes the following functionalities:

Configuring communication gateways.

Users select how Babelgom will communicate with external systems A and B. The communication protocol used with system A can of course be different from the communication protocol used with system B. Users can choose amongst the following communication protocols:

AS2 : this a communication standard largely used in retail to secure communication over the Internet.

Ftp client : to set-up an FTP client accessing an external FTP server

Ftp server : to configure the Ftp server receiving incoming messages or to place outgoing messages

Email : to set-up a new Email address to receive incoming messages or to send outgoing messages

Fetch Mail : this is used to retrieve messages from an external POP3 mailbox

Web gateway : to set-up a website access to upload incoming messages or to download outgoing messages

SOAP gateway : to set-up a SOAP gateway (SOAP client) to send outgoing messages to a SOAP server.

Once the communication technology is selected, users fill in the template with the technical parameters that will be used to establish the connection between Babelgom and the external system.

If certificates are an element of the communication protocol (eg. AS/2 or FTPs), users will incorporate the external system certificate as a technical parameter. Users will provide the corresponding Babelgom certificate to the external system. (See the relevant chapter for details of security and certificate management)

Note: each Babelgom user has its own set of gateway addresses or locators. External systems are therefore connected to individual Babelgom users, not to Babelgom in general.

Defining a message format.

Users select the format amongst the following options

CSV : to define a character delimited flat file with constant record definition (data are in columns)

EDIFACT : to define a new message in EDIFACT format

X12 : to define a new message in X12 format

MS Excel : to define a new message in MS Excel ('97 to '03)

Users will then upload an example of a message in this format. The system will automatically provide an XML version as well as a visual representation in a hierarchical tree structure.



XML can also be selected. In this case, users upload an example or the XSD file. For custom flat file formats (eg. Fixed length or multi-records), users should also upload a specific configuration file built using ServingXML library.

Creating a new message format (not supported by Babelgom) : advanced users have the option to upload programmatic code that enables the support to proprietary messages formats, such as specific binary ERP format (eg. idoc of SAP).

Creating transformation rules between the message IN and the message OUT.

Users can create the transformation rules using the drag&drop interface tool. Users can create correspondences between the message IN and the message OUT by dragging and dropping message fields from left to right.

For more complex transformation operations, users have a portfolio of standard operations they can call upon (concatenation, date formatting, etc.). More advanced users can also define new standard operations using the xpath syntax.

In some cases, advanced users will prefer to depart from the visual drag&drop interface and work directly in the underlying XSLT structure, which is less user-friendly but can prove quicker for XSLT developers.

Creating validation rules

Users can define validation rules to be applied on incoming and/or outgoing message. Validation can for example make the presence of values in some fields mandatory or make them correspond to a pre-set of values. Validation is particularly useful to prevent that an external system received messages that it cannot process automatically.

Signing outgoing messages

Users can configure channels such that outgoing messages are signed using a dedicated advanced certificate and if the outgoing format enables such signature (must be PDF or ZIP format). (See the relevant chapter for details of security and certificate management).

Creating lookup tables

Users can define and load tables of values, called lookup tables, which are used during the transformation process to change an incoming value into a corresponding outgoing value. An illustrative application of lookup tables is to enable a buyer and a supplier to use different product codes to identify similar products (eg. GTIN codes versus internal codification).

Building test cases

Users can build test cases of their channels. The test cases enable the user to check the result of its work on message formats and transformation prior to deploying a channel into the production environment.

Managing routing across channels

Messages originating from a common source but going to various external systems must be routed. Users can define routing rules based on message content items or on message context.

Managing notifications

For each channel individually, users can build automatic notifications that will send an email to a specified address upon the arrival of a new message. Notified users can be different if the message is successfully processed or generated an error.

Avoiding rework thanks to the catalogue

Gateway parameters, message formats, transformation and validation rules are created during the channel building process. Each of these items can be re-used in the building of a subsequent channel. This is organized via what we call the catalogue where all new items are listed.

Users populate a new channel from the items available in their catalogue. This catalogue enriches itself progressively each time new channels are built. When users decide to source an item from the catalogue, they make a choice to use the same instance or to duplicate it. This choice is important when making changes to channels. If channels share the same instance of an item, a change in one channel will impact all other channels using the same item.

Note: Babelgom will soon enable users to open up their catalogue to other selected Babelgom users, such that channel items created by one user can be re-used by another user. Functionalities will include the secure management of access rights, the possibility to charge for the use of catalogue items and the possibility to track and measure usage of catalogue items.

Activating and deploying channel updates

Users decide which channels are under construction and which must be activated upon deployment in the production environment of Babelgom.

Tracking messages

Messages that flow through the user hub can be tracked and traced. Users have access to any message stored, in all its forms (before, during and after transformation) together with contextual information such as time of entry, time of exist, status, as well as relevant security-related information such as certificates and signatures.

Managing tickets

Multiple events generate tickets. For example, processing issues of a message generate tickets. Tickets provide detailed information to users as well as tools to manage resolution. Messages that are in error can be accessed directly for manual correction and resubmitted in a channel.

Account management

The account management function includes the following services:

Adding/modifying/deleting users with access to individual user hubs.

The administrator of an account can provide access to one of its hub to other users. Access rights can be

- Account Administrator : Full rights over the account.
- Hub User : Full rights over tickets/messages/channels/catalogue functions of the hub, cannot modify account information, subscription parameters, other user rights. This type of access is for people who will manage and maintain all data exchanges, without being allowed to view and change specific account information.
- Catalogue User : Rights to view and import catalogue items of the hub into another Babelgom hub. Cannot access any other functions, cannot modify anything. This type of access is for people allowed to source catalogue items from a hub for re-use in their own Babelgom hub.
- Web Gateway User : Can upload/download messages from the specific webpage of the hub. Cannot view or access anything else than messages from/to them. This type of access is for people who will manually upload/download message files.

Creating/modifying/deleting individual user hubs.



An account can be made of any number of different hubs. It can be useful to build channels in separate hubs if

- different people should have access rights; or
- message storage duration should be differentiated; or
- performance expectations are different
- security requirements imposes it

Buying usage units in the Babelgom online shop and viewing the financial status of the account. This feature is currently under development.

Performance management

Each hub has a default processing capacity. The default processing capacity is allocated by Babelgom to meet the default service level agreement towards users.

Users can increase the processing capacity in multiple increments of the default processing capacity. By doing this, users can double, triple, quadruple, etc. the processing capacity of their hub and therefore handle very large amount of simultaneous data flows, without depending of the general consumption of capacity in other Babelgom hubs.

Storage management

As a default option, Babelgom stores messages for a period of 3 months. Users can select the 'long-term archiving' option which provides storage for any period of time up to 12 years.

Other terms of storage (shorter or longer) could be accommodated with individually.

CHAPTER 2: QUALITY AND SECURITY MANAGEMENT

Hosting and redundancy

Babelgom infrastructure is hosted externally. Babelgom has contracted with 2 hosting providers:

- Combell, a recognized Belgian hosting company. Combell uses the physical premises of LCL, located in Diegem, Belgium. Premises have been audited by an independent consultant mandated by Babelgom.
- Amazon, a recognized International company. Babelgom subscribes to the Amazon Web Service (AWS) offering whereby Babelgom has access to virtual servers "on-demand". Servers are physically located on the US and UK territory.

To maximize availability and reliability, not only has Babelgom contracted on strict terms with reliable partners, but Babelgom has installed redundancy between its 2 data centers. In case of downtime of one of the 2 data centers, Babelgom can switch all data traffic to the other data center.

Limitations of the redundancy are:

- Web interfaces (human access to user hubs) are located with Combell only. In case of unavailability of the Combell infrastructure, messaging services can continue but human tracking or maintenance is not available .
- Gateways to external systems based on physical IP addressing would also be interrupted. We recommend users to use URL locators instead of IP addressing wherever possible.

Note: this approach technically allows customers of Babelgom to host their messaging themselves while still using the unique Software-as-a-Service. This could be important to some customers if security reasons require customers to control the messaging servers themselves or to have servers physically located in some specific geographic territory, for example.

Infrastructure management

Our hosting providers have demonstrated to Babelgom that they managed infrastructure according to our (ISO 27001) expectations levels.

Amazon AWS security processes are described on <http://aws.amazon.com>. Babelgom subscribes to EC2 and S3 services. Amazon AWS has the security certification SAS70 type II. Amazon cannot access Babelgom data in any way. All data communication, storage and back-ups are encrypted. Encryption is made using a 2048bits private key created by Babelgom and stored on Babelgom server file system, with access restricted to the super user (root), a member of Babelgom management.

Combell security processes are described on <http://www.combell.com/en/>. Babelgom has contracted dedicated physical servers with Combell. Combell staffs don't have access privileges to Babelgom servers.

Software management

Babelgom software development are in Java (J2EE) programming language.

Babelgom has assembled open source and proprietary package software. Just to mention some, we use JBoss ESB as the core messaging engine, EDIReader as EDIFACT to XML converter, ServingXML as customer flat file to XML converter, Hermes as AS/2 platform, Postgres as database.

These components have been integrated in a very large development programme that started in October 2006. Our technical developments are centrally managed from our base in Belgium. We



made extensive use of very acute expertise on highly specific topics such as scalability, database optimization, ergonomics, cryptography, processing performance, XML and EDIFACT standards, etc with recognized specialists in each of these fields and usually for short, highly focused mission. We also used off-shore development partners to execute portions of code programming during the peak development period.

Software development follows a very strict quality process, fully documented and compliant to ISO27001 guidelines (see below).

Data security and traceability

Babelgom software strictly controls data access using isolation techniques. This ensures the total data independence between hubs. All accesses to hub and customer data are logged in an audit trail.

Monitoring

Monitoring of systems and applications are performed using different mechanisms.

- An internal monitoring tool based on Hyperic HQ is used to test the availability and performance of the different components of the system.
- An external monitoring tool (InternetVista) is used to test the availability and the performance of the Web interfaces and the system gateways.
- A positive & reactive monitoring alert is triggered when a situation requires human intervention (for instance, a message entering the system and not processed within 5 minutes)

All tools are collecting information, generating statistics and deliver alert if needed. Issues and bugs encountered are logged and tracked for further reference and follow up.

Human monitoring is also performed on the application console and logs in order to track and analyze overall behavior of the platform. Monitoring and general maintenance tasks are documented in an Operations Manual which is a key component of the Security Policy. Attacks and odd behaviors detected by any kind of monitoring are documented and tracked in the security breach and incident reports. Capacity planning is part of the monitoring and a process is in place to review overall capacity requirements on a monthly basis.

ISO27001 and quality management

Babelgom has put in place an Information Security Management System (ISMS) compliant to ISO27001 guidelines. Babelgom's policy regarding security can be consulted on-line (<http://www.babelgom.com/security-policy.php>) . The system ensures processes are in place to meet the policy's objectives.

Security Certificates

Babelgom uses the following security certificates:

Babelgom qualified certificate

Babelgom uses the Belgian electronic identity card (eID) of designated members of the Board of Directors of Babelgom as the Babelgom qualified certificates of Babelgom. The Babelgom qualified certificate is used in signing chain timestamps in the message archives.

User hub advanced certificates

A pair of "root" keys is generated by Babelgom for each user hub on a secure machine, not connected to the network. The public key is included in a self-signed "root" user hub certificate and stored in the hub keystore. The private key remains in a separate keystore on the secure machine.

The user hub certificate is sent to the Babelgom security hub and stored as any other message, guaranteeing its integrity and timestamping (see archiving section below)



Babelgom creates 3 pairs of keys of each hub and, using the user hub root certificate, associates them with 3 hub certificates:

- a transfer pair, generated on the secure machine and stored in the keystore of the user hub. This certificate can be used by customers to sign outgoing emails with structured file attached (EDI method) or to sign PDF or ZIP file that encapsulate a message and sent via unsecure network (e-signature method)
- a storage pair, generated on the secure machine and stored on the user hub. The public key is included in a storage certificate signed by the user hub root certificate. This certificate is used systematically to sign all stored messages of the user hub.
- An encrypting pair, generated on the secure machine and stored on the user hub. The public key is included in an encryption certificate signed by the user hub root certificate. This certificate is used systematically to encrypt all stored messages of the user hub.

Babelgom SSL certificate

Secure transfer certificate, associated with Babelgom servers and certified by Thawte (Verisign). This certificate guarantees authenticity and confidentiality for exchanges using protocols: Web (https), SOAP (https), FTPs and FTPs Servers, AS/2 (https layer), whatever the customer hub performing the document exchange.

Babelgom SSH certificate

Secure transfer certificate, used for exchanges using the sFTP protocol. This certificate is self-generated by Babelgom with Babelgom as root authority. The certificate is 'manually' accepted by the exchange partner during the set-up of the sFTP connection.

Babelgom AS/2 certificate

Secure transfer certificate, used for exchanges using the AS/2 protocol. This certificate is self-generated by Babelgom with Babelgom as root authority. The certificate is 'manually' exchanged between partners during the set-up of the AS/2 connection.

In addition to Babelgom certificates, users can include/exclude external systems certificate in their own trusted certificate list (keystore).

Keystore management

Each user hub has its own keystore. This keystore keeps all the keys and certificates necessary for the runtime of the hub. It also contains the trusted external systems certificates. Users can add or delete trusted certificates. Users have no access to user hub private keys.

The keystore is based on recognized cryptographic standards. Access is protected with a password system with multiple layers.

Transfer security

Users have multiple options to send outgoing messages securely.

- They can use a protocol secured with one (or more) network certificate (SSL, SSH or AS/2).
- They can sign outgoing messages (PDF or ZIP formats) with their user hub transfer certificate (under construction)
- They can sign emails with their user hub transfer certificate (under construction).

Archiving security

Each flow of message through a Babelgom channel creates multiple files:

- the message as it existed when entering a channel of the user hub;
- the message as it existed when exiting a channel of the user hub;



- possible intermediary (XML) versions of the message between entry and exit.

A flow through a single channel creates a single 'message record' where individual files and their signatures are grouped.

The following process is used to guarantee the integrity of the stored files.

All files are individually signed using the storage certificate of the user hub using the SHA512 and RSA algorithms. The signature is hashed (SHA512) and the result is kept for the chain mechanism described below. The file is then encrypted with the encryption certificate of the user hub using the AES256 algorithm. (Optionally, users can upload an encryption key that is used to encrypt stored files, in this case, encrypted files would be signed again with the user hub storage certificate). The encrypted file and its signature(s) are then stored.

For each stored file, there is the following contextual data:

- an ID (sequence number)
- the date and time of the storage
- the "hash" of the signature created with the storage certificate
- the user hub ID number
- hash of the contextual data of the previously stored message

At regular intervals, Babelgom signs the hash of the contextual data of the last available message with its qualified certificate. This is timestamped by the timestamp authority of the Belgian Federal government. At the same time, Babelgom requests a validity proof for the Babelgom qualified certificate from the Belgian authority (Citizen CA).

The chain makes it impossible for an individual user or for Babelgom to change any stored element without breaking the chain and therefore making it detectable.

Proving authenticity of origin and integrity

Users of Babelgom can demonstrate the authenticity of origin and the integrity of messages flowing through their hub as follows:

In case users use the transfer certificate, the public key or its footprint of their "root" hub certificate must be included in the interchange contract that Babelgom users sign with their business partners. This explicitly shows the agreement of the parties to trust exchanges between themselves using this specific Babelgom user hub certificate. It should be noted that :

- The fact that user hubs on Babelgom are unrelated to each other (no common certification authority) brings additional security in the sense that accepting exchanges with one Babelgom hub doesn't imply accepting exchanges with all Babelgom hubs. Each B2B relationship must be individually certified between the parties. Users have the responsibility to inform their business partners of changes in the validity of their certificates.
- The absence of trusted Third-Party has no incidence on the validity of the signature as an advanced signature. The Parties have certified the identity of their counterpart through the interchange agreement (bilateral agreement).
- The chain mechanism in the storage system of Babelgom guarantees (to users as well as to the tax administration, for example) that messages have not been tampered with by anyone, including Babelgom.

To verify the authenticity and the integrity of a specific file:

- The message record page in the user hub includes the decrypted file, the hash of the signature, the certificate of the storage public key of the user hub, the sequence number of the file, the sequence number of the user hub root certificate, the previous and next authenticated timestamp
- The previous and next authenticated timestamp must be verified
- The chain is recreated between the 2 timestamps by re-hashing the contextual data of each stored file. This certifies the stored hash of the storage signature.
- The conformity of the message is verified. In particular,



- the signature hash should be recalculated and checked against the stored hash for the message.
- Check the signature of the storage key by the root certificate
- Check the presence of the root certificate in the storage system and its conformity following the same process
- Check the signature

This verification process guarantees that

- The message has been processed by a specified user hub on Babelgom
- At the date that is claimed
- The message has not been modified since its signature

Audits and external qualifications

From May to October 2008, Professor Jos Dumortier, internationally recognised expert in the field of the legal electronic signature, audited the Babelgom solution and checked its compliance with the legal requirements imposed by the EU Directive about electronic invoicing. Professor Jean-Jacques Quisquater, cryptographic expert, assisted in the project to provide an opinion about the specific use of cryptographic technologies made by Babelgom.

The project resulted in an audit report that concludes that Babelgom meets the legal obligations regarding e-invoicing. The signature made available to Babelgom customers is indeed an 'advanced signature' in the legal sense since it fulfils the 4 conditions, namely:

- It is uniquely linked to the signatory
- Identifies the signatory
- Is created by means that the signatory can keep under its sole control
- Is linked to the data in such a way that any change is detectable

Note: Babelgom offers an 'advanced signature' to transfer and store messages. Customers can use Babelgom in a way that can guarantee authenticity of origin and guarantee of integrity. However, Babelgom doesn't take responsibility for the way customers assemble specific channels, establish interchange contracts with their partners and link up their own systems with their Babelgom hub. Babelgom stresses to customers that it belongs to them to check their own usage of Babelgom and to assess whether it copes with their local regulatory environments.



CHAPTER 3: USER SUPPORT

Community Forum

Users can consult and interact with Babelgom and other users through the community Forum, available to registered users from their web interface at www.babelgom.net. This forum addresses any questions users may have. Answers are made generally available for future reference.

Helpdesk

The human monitoring function provides helpdesk support to users via email and telephone on business day from 9:00 to 18:00.

Support partners

Babelgom develops partnerships with IT support companies to provide specialized support for some applications or in some industries or territories. Babelgom partners are listed on the Babelgom website at <http://babelgom.com/data-exchange-partner.php>.

Training : BABEL ACADEMY

Babelgom organizes training sessions at regular intervals. The calendar, program and conditions can be requested at info@babelgom.com