



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

**White Paper**  
BABELWAY 2.0

October 2008

### Contents

INTRODUCTION.....	2
EXECUTIVE SUMMARY.....	3
CHAPTER 1: FUNCTIONALITIES OVERVIEW.....	4
CHAPTER 2: QUALITY AND SECURITY MANAGEMENT.....	10
CHAPTER 3: USER SUPPORT.....	16



## INTRODUCTION

The benefits to businesses of EDI in general and e-invoicing in particular have been widely documented in multiple reports. An EC report<sup>1</sup> quotes 238 billion Euros, 400,000 tons of paper, 2,700 tons of ink, 160 million litres 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.

### The 2 traditional EDI methods

The 2 traditional methods of automating 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 most historically common method. Companies buy (or custom build) and install a B2B communication system within a company's internal IT environment and organise 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 a significant investment in money, time and skills. Larger companies have traditionally opted for this method.

Together with the internet, a second method of carrying out EDI emerged: the B2B integration hub. Point-to-point communication is replaced by a central hub which means that one communication to the central hub is sufficient to reach all other partners. The B2B integration hub enables one to communicate rapidly with a community of trading partners. The value proposition of the B2B integration hub is to create a single technical link between an individual company and the hub. B2B data flows will then be technically organised 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 the time comes to connect to a new business partner. Medium-sized companies have usually chosen this method.

What's different about Babelway?

Babelway B2B integration Software-as-a-Service has bridged the 2 traditional methods. Babelway enables customers to connect directly to their partners, avoiding the need for B2B intermediaries. Customers therefore have complete **control** over their data flows. In addition, Babelway does not 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 Babelway users can share common components of data flows (e.g. the invoice format of Carrefour Belgium) through a catalogue of components which leads to a decrease in the time it takes to build new channel as the community increases.

Babelway 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 Babelway. It is addressed to those carrying out an in-depth evaluation of an EDI and e-invoice solution. We also advise these people to register online now to freely discover for themselves what Babelway can do and how it works.

---

<sup>1</sup> « 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](http://ec.europa.eu/information_society/eeurope/i2010/docs/studies/eei-3.2-e-invoicing_final_report.pdf).



## EXECUTIVE SUMMARY

Babelway B2B integration Software-as-a-Service allows organisations to automate cross-company processes and enables the secure exchange of structured and recurrent documents such as orders invoices, payslips, reports, payment advices, etc.

All it takes to be ready to automate data exchange with ANY business partner or computer application is to register online ([www.babelway.net](http://www.babelway.net)) . Babelway guarantees foolproof security, unlimited scalability and first-class performance. Babelway is the solution for rapidly connecting to a trading community while still retaining full control over data flows.

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

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

Babelway software and infrastructure is managed using the strictest quality and security management processes. At the time of writing, Babelway was in the process of ISO27001 certification that provides the management system to ensure total security in highly technical environments. Babelway is hosted in 2 redundant data centres. All systems are permanently monitored by internal and external systems. Storage is encrypted to guarantee confidentiality. Babelway 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 Babelway solution has been audited and qualified as compliant with the relevant EU regulation by Professors Dumortier (KUL) and Quisquater (UCL), internationally recognised experts in the fields of electronic signature and cryptography.

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

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



## CHAPTER 1: FUNCTIONALITIES OVERVIEW

Babelway is the first B2B integration Software-as-a-Service. Babelway provides EDI translation software and B2B communication gateways organised in a full-service proposition. Babelway services are fully available on-demand via a web-browser. There is no software or hardware to buy and maintain in-house, but yet Babelway is still under the full control of its 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 Babelway in order to organise an automatic data flow from an external system A to another external system B. The key components are

- (1) the way in which Babelway is interfaced with system A, called the “gateway IN”,
- (2) the way in which 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 in which Babelway is interfaced with system B, called the “gateway OUT”

Welcome fvanuffelen42 | My Account | Log Out | Community Forum | +32 (0)10 390 013

Tickets Messages Channels

Edit Channel

Successfully created

Back Duplicate channel Delete Activate

General Gateway In Message In Transformation Message Out Gateway Out Email Notifications Routing Testing

Id 32888

Name

Description

Status Off

Last Updated On 23/04/2009 21:13CEST

Last Deployed On

Next Deployment No Change

Save

\* Required fields to activate the channel

In building channels, Babelway contains the following functionalities:

### Configuring communication gateways.

Users select how Babelway 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 from 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

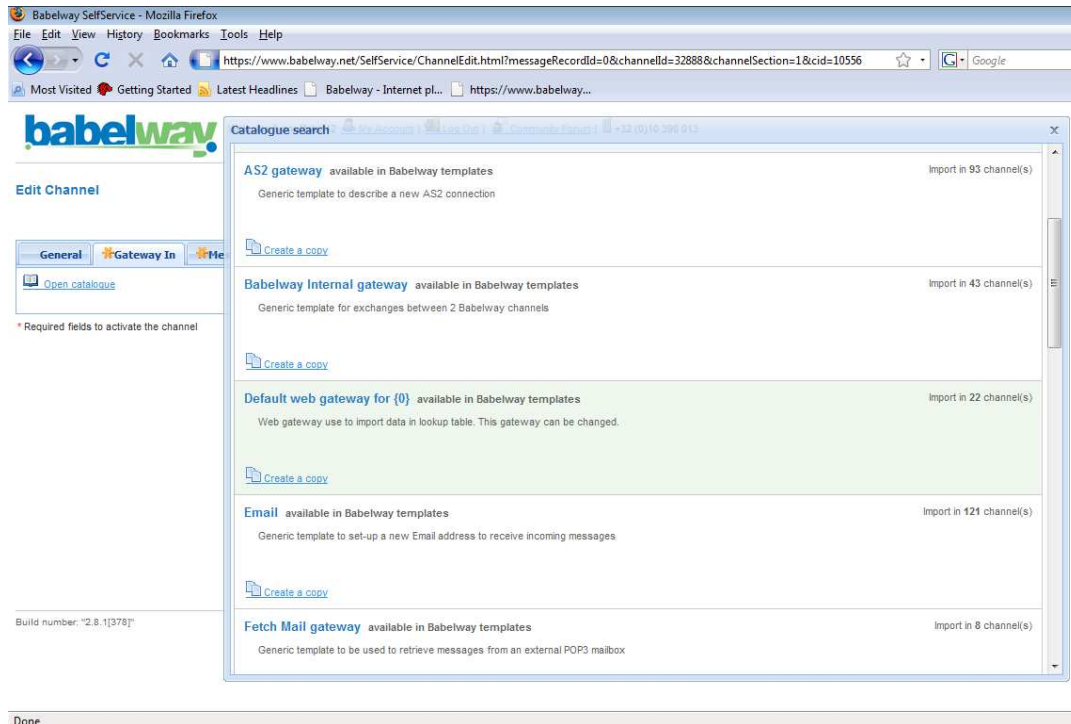
Ftp server: to configure the FTP server receiving incoming messages or to place outgoing messages

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 has been selected, users then fill in the template with the technical parameters that will be used to establish the connection between Babelway 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 Babelway certificate to the external system. (See the relevant chapter for details of security and certificate management)

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

### **Defining a message format.**

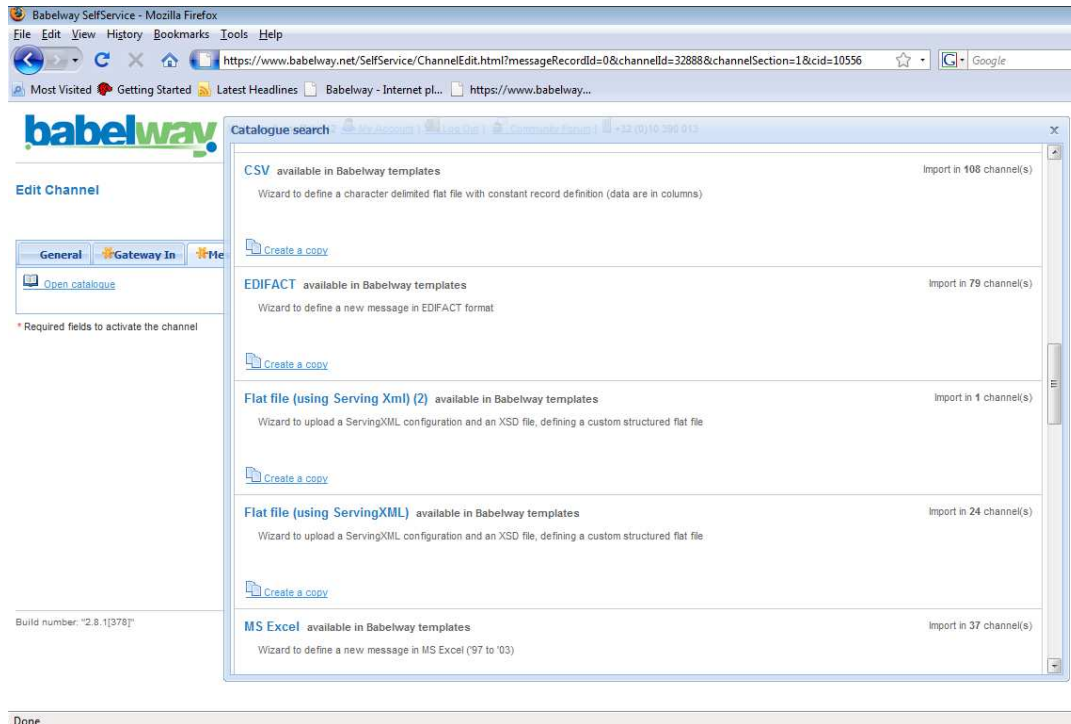
Users select the format amongst the following options

CSV: to define a character-delimited flat file with constant record definition (data is 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 (e.g. Fixed length or multi-records), users should also upload a specific configuration file built using ServicingXML library.

Creating a new message format (not supported by Babelway): advanced users have the option to upload programmatic code that provides support to proprietary messages formats, such as specific binary ERP format (e.g. 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 messages. For example, validation can 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 look-up tables, which are used during the transformation process to change an incoming value into a corresponding outgoing value. An illustrative application of look-up tables is to enable a buyer and a supplier to use different product codes to identify similar products (e.g. GTIN codes versus internal codification).

### **Building test cases**

Users can build test cases of their channels. The test cases enable users to check the result of their 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 individual channel, 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 an error is generated.

### **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 organised via what we call the catalogue, the place 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: Babelway will soon enable users to open up their catalogue to other selected Babelway users, so 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 of charging for the use of catalogue items and the possibility of tracking and measuring the 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 Babelway.

### **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.



## List of Messages (1932)

Message Search

Date In	Gateway In	Channel	Gateway Out	Size [B]	Message Reference	Status (Acknowledged)
17/12/2008 11:15:27 CEST	phone-house-upload	DESADV	AS2 Carrefour	1949	060459_D...17110224	Success (Ack)
17/12/2008 10:15:27 CEST	phone-house-upload	DESADV	AS2 Carrefour	25338	060458_D...17101433	Success (Ack)
17/12/2008 02:00:38 CEST	phone-house-upload	INVOICE Splitter	Splitter	4054	CARRE4IN...00000876	Success
17/12/2008 02:00:38 CEST	phone-house-upload	INVOICE Splitter	Splitter	404	CARRE4IN...00000874	Success
17/12/2008 02:00:38 CEST	phone-house-upload	INVOICE Splitter	Splitter	404	CARRE4IN...00000873	Success
17/12/2008 02:00:38 CEST	phone-house-upload	INVOICE Splitter	Splitter	550	CARRE4IN...00000871	Success
17/12/2008 02:00:28 CEST	phone-house-upload	INVOICE Splitter	Splitter	550	CARRE4IN...00000870	Success
16/12/2008 17:52:58 CEST	phone-house-upload	DESADV	AS2 Carrefour	13300	060669_D...16163944	Success (Ack)
16/12/2008 15:45:20 CEST	phone-house-upload	DESADV	AS2 Carrefour	1949	060667_D...16153818	Success (Ack)
16/12/2008 15:01:50 CEST	phone-house-upload	DESADV	AS2 Carrefour	13966	060626_D...16145412	Success (Ack)
16/12/2008 14:00:21 CEST	phone-house-upload	DESADV	AS2 Carrefour	21324	060459_D...16135856	Success (Ack)
16/12/2008 13:30:21 CEST	phone-house-upload	DESADV	AS2 Carrefour	1949	060669_D...16132604	Success (Ack)
16/12/2008 13:30:20 CEST	phone-house-upload			40		Success (Ack)
16/12/2008 13:16:51 CEST	phone-house-upload			65		Success (Ack)
16/12/2008 11:30:20 CEST	phone-house-upload			40		Success (Ack)
16/12/2008 11:15:23 CEST	phone-house-upload			1		Success (Ack)
16/12/2008 11:15:23 CEST	phone-house-upload			9		Success (Ack)
16/12/2008 11:15:22 CEST	phone-house-upload			65		Success (Ack)
16/12/2008 10:45:20 CEST	phone-house-upload	DESADV	AS2 Carrefour	15980	060632_D...16103724	Success (Ack)
16/12/2008 02:00:21 CEST	phone-house-upload	INVOICE Splitter	Splitter	404	CARRE4IN...00000867	Success
15/12/2008 20:16:41 CEST	phone-house-upload	DESADV	AS2 Carrefour	1951	060632_D...15200139	Success (Ack)
15/12/2008 19:01:42 CEST	phone-house-upload	DESADV	AS2 Carrefour	1949	060632_D...15184754	Success (Ack)
15/12/2008 15:16:41 CEST	phone-house-upload	DESADV	AS2 Carrefour	17316	060606_D...15150000	Success (Ack)
15/12/2008 14:31:41 CEST	phone-house-upload	DESADV	AS2 Carrefour	13972	060664_D...15142020	Success (Ack)
15/12/2008 14:16:41 CEST	phone-house-upload	DESADV	AS2 Carrefour	1951	060632_D...15140911	Success (Ack)

With AS2 protocol, users receive the status 'ack' as well as the MDN key

Next Page > Last Page >>

## Message Record

Message Record Id	174480
Message Id	174480
Date In	17/12/2008 11:15:27 CEST
Date Out	17/12/2008 11:15:27 CEST
Gateway In	phone-house-upload
Channel	DESADV
Gateway Out	AS2 Carrefour
Gateway Out	20081217-111527-40222691.1958.243.66
Message Key	
Gateway Out	Processed (mdn id: 4CAA623045-A2642AC511-0A58CAD4F5-B5F7A041D6@C4NETBE_host)
Message Status	
Acknowledgment Reference	4CAA623045-A2642AC511-0A58CAD4F5-B5F7A041D6@C4NETBE_host
Size [B]	1949
Output size	1949
Message Reference	060459_DESADV0000641958.20081217110224
Status	Success
Message Type	Regular
Message In	<a href="#">060459_DESADV0000641958.20081217110224</a>
XML In	<a href="#">060459_DESADV0000641958.20081217110224.xml</a>
XML Out	<a href="#">060459_DESADV0000641958.20081217110224.xml</a>
Message Out	<a href="#">060459_DESADV0000641958.20081217110224</a>
Context	<a href="#">context.txt</a>

By clicking on the message, users view the message record, including all AS2 details

[Back](#) [Save As Test Case](#) [Resolve](#)

## Managing tickets

Multiple events generate tickets. For example, processing issues related to a message generate tickets. Tickets provide detailed information to users, as well as tools for resolution management. 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 other users with access to one of its hubs. Access rights are as follows:



- 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 Babelway 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 Babelway 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 up 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 demand it
- there is a need for a test environment

Buying usage units in the Babelway 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 Babelway to meet the default service level agreement towards users.

Users can increase their 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 being dependent on the general consumption of capacity in other Babelway hubs.

### **Storage management**

As a default option, Babelway 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) may be accommodated individually.



## CHAPTER 2: QUALITY AND SECURITY MANAGEMENT

### Hosting and redundancy

Babelway infrastructure is hosted externally. Babelway has agreements with 2 hosting providers:

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

To maximise availability and reliability, not only has Babelway contracted on strict terms with reliable partners but it has also installed redundancy between its 2 data centres. In the event of downtime of one of the 2 data centres, Babelway can switch all data traffic to the other data centre.

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 that users use URL locators instead of IP addressing wherever possible.

**Note:** this approach technically allows customers of Babelway to host their messaging themselves while still using the unique Software-as-a-Service. This could be important to some customers if security considerations require them 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 Babelway that they managed infrastructure according to our (ISO 27001) expectations levels.

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

Combell security processes are described at <http://www.combell.com/en/>. Babelway has an agreement with Combell for dedicated physical servers. Combell employees do not have access privileges to Babelway servers.

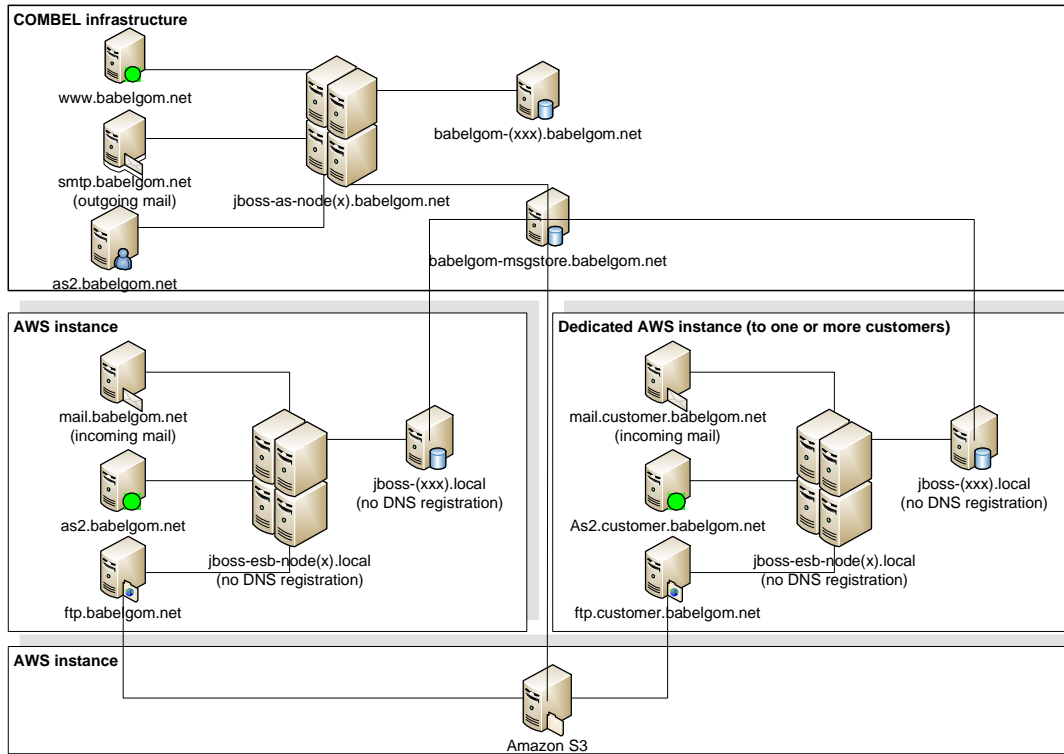
The components (database, application server, gateways, etc.) of the infrastructure within each data centre have their own fail-over mechanism.

Failover between the 2 data centres is organised as follows:

Babelway always maintains the configuration of the 2 data centres in sync. All customer configurations are deployed concurrently on both infrastructures. The load balancing and the fail-over between data centres are performed at the DNS level. The messaging engine deployed in the 2 data centres have the ability to work in complete autonomy in both active / active or active / passive modes. This mechanism is used by Babelway for fail-over as well as scalability needs. To fully leverage Babelway fail-over mechanism, traffic with Babelway gateways should either be based on DNS (logical addressing) or accept a pool of IP addresses (those of both data centres).



Here under, the high level deployment view of Babelway messaging engine infrastructure, showing how the two data centres are interacting.



## Software management

Babelway software development is in Java (J2EE) programming language.

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

These components have been integrated into an extensive development programme which began in October 2006. Our technical developments are centrally managed from our base in Belgium. We have made extensive use of very precise expertise on highly specific topics such as scalability, database optimisation, ergonomics, cryptography, processing performance, XML and EDIFACT standards, etc with recognised specialists in each of these fields and usually for short, highly focused missions. We have also used off-shore development partners to carry out portions of code programming during the peak development period.

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

## Data security and traceability

Babelway 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

The monitoring of systems and applications is 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 remaining unprocessed for more than 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 analyse the overall behaviour 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 behaviour 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**

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

## **Security Certificates**

Babelway uses the following security certificates:

### **Babelway qualified certificate**

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

### **User hub advanced certificates**

A pair of "root" keys is generated by Babelway 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 Babelway security hub and stored as any other message, guaranteeing its integrity and timestamping (see archiving section below)

Babelway creates 3 pairs of keys for 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 a structured file attached (EDI method) or to sign PDF or ZIP files that contain a message and are sent via an unsecured 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.

### **Babelway SSL certificate**

Secure transfer certificate, associated with Babelway 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.

### **Babelway SSH certificate**

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

### **Babelway AS/2 certificate**

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

In addition to Babelway 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 recognised cryptographic standards. Access is protected with a password system with multiple layers.

## **Transfer security**

Users have multiple options in order to securely send outgoing messages.

- 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 Babelway 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 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, Babelway signs the hash of the contextual data of the last available message with its qualified certificate. This is time-stamped by a trustworthy timestamp authority. At the same time, Babelway requests a validity proof for the Babelway qualified certificate from the Belgian authority (Citizen CA).

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

## **Proving authenticity of origin and integrity**

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

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

- The fact that user hubs on Babelway are unrelated to each other (no common certification authority) provides additional security in the sense that accepting exchanges with one Babelway hub does not imply accepting exchanges with all Babelway hubs. Each B2B relationship must be individually certified between the parties. Users are responsible for informing their business partners of changes in the validity of their certificates.
- The absence of a trusted third party has no influence 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 Babelway guarantees (to users as well as to the tax authorities, for example) that messages have not been tampered with by anyone, including Babelway.

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

This verification process guarantees that

- The message has been processed by a specified user hub on Babelway and on the date which is stated
- The message has not been modified since its signature

## **Audits and external qualifications**

From May to October 2008, Professor Jos Dumortier, an internationally recognised expert in the field of legal electronic signatures, audited the Babelway solution and checked its compliance with the



legal requirements imposed by the EU Directive about electronic invoicing. Professor Jean-Jacques Quisquater, an expert in cryptography, assisted in the project by giving his views on the specific use of cryptographic technologies made by Babelway.

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

- It is uniquely linked to the signatory
- It identifies the signatory
- It is created in such a way that the signatories can maintain it under their sole control
- It is linked to the data in such a way that any change is detectable

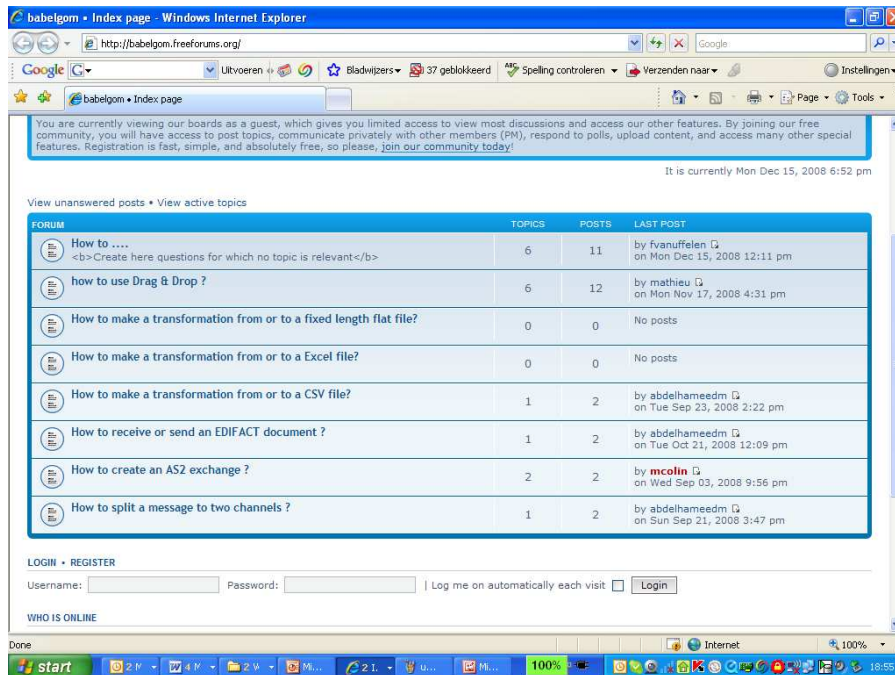
Note: Babelway offers an 'advanced signature' to transfer and store messages. Customers can use Babelway in a way that can guarantee the authenticity of origin and the integrity of the message. However, Babelway does not accept responsibility for the way in which customers assemble specific channels, establish interchange contracts with their partners and connect their own systems to their Babelway hub. Babelway stresses to customers that it their responsibility to check their own usage of Babelway and to assess whether it is compatible with their local regulatory environments.



## CHAPTER 3: USER SUPPORT

### Community Forum

Users can consult and interact with Babelway and other users through the community Forum which is available to registered users via their web interface at [www.babelway.net](http://www.babelway.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 working days from 9am to 6pm.

### Support partners

Babelway develops partnerships with IT-support companies in order to provide specialised support for certain applications or in certain industries or territories.

### Training: BABEL ACADEMY

Babelway organises training sessions at regular intervals. The calendar, program and conditions are available from our website [http://www.babelway.com/babel\\_academy.php](http://www.babelway.com/babel_academy.php)