iQ.Suite Bridge

- Legally compliant email archiving and compliance interface -

Expertise matters

Contents

1 Background

Email is one of the most important communication media for both business and private data. Today, emails are used to initiate, conclude and conduct business, as well as to maintain contact between customers and suppliers during the term of the contract.

The law contains a series of requirements setting out how emails should be used in the context of business correspondence. Other requirements concern the use of emails in communication with Support, and the storage of emails in downstream CRM and ERP systems, and in other systems.

This whitepaper shows how iQ.Suite Bridge can help you to configure your requirements, whether in the field of archiving, data storage or data structuring.

2 Introduction

The explosive increase in the use of emails is not only a challenge for email systems, it is an increasing burden on the resources and infrastructure of many companies. Emails not only occupy disk space, they need to be organised properly, too. For example, private and business content needs to be separated and classified.

In a company, inbound and outbound emails must be regarded as business correspondence and dealt with accordingly. Business correspondence must be managed, it must be traceable, and it must be archived in a manner that complies with audit regulations. A whole series of proprietary guidelines and statutory regulations, e.g. the GDPdU in Germany and the SEC regulation in the USA, demand a centralised, rule-based compliance and archiving solution for emails. iQ.Suite Bridge is more than an archiving interface. Bridge is the compliance interface you need to integrate emails into your internal business processes and thus establish an effective email management system.

An integral part of iQ.Suite Bridge is a flexible module for exchanging data and information between a messaging platform and business applications. It does this by providing the relevant business applications with email data and by processing the control sequences of these business applications on the messaging platform.

What Bridge can do:

- Bridge connects your messaging platform with archiving systems, and compliance, CRM, DMS and/or ERP systems
- Bridge seamlessly integrates business-critical emails into your business processes
- Bridge avoids the need for user intervention, thus preventing deliberate or accidental tampering

3 Legal Requirements

In many companies, email management is restricted to direct actions such as repelling spam and viruses, with scant regard for how electronic correspondence should be handled in the long-term. But the law requires companies to treat emails, i.e. digital documents, as if they were conventional commercial documents and to preserve them for a specific period of time. Connecting the email system to an archiving system should, therefore, be a matter of top priority for a company so that all email traffic can be documented in an audit-compliant manner. But many companies fail to archive their emails at all or leave the task to their employees, something which inevitably leads to flawed and incomplete records. Essential guidelines on archiving emails are often lacking in many companies.

3.1 What Are the Relevant Laws?

In Germany, the Fiscal Code, the Generally Accepted Accounting Principles, the Principles for Accessing Data and Verifying Digital Documents, the Commercial Code, and the Generally Accepted Principles of Computerised Accounting Systems govern the archiving of emails. In the USA, SEC Rule 17a-4, HIPPA, the provisions of the NASD for the financial community and, since 2002, the Sarbanes-Oxley Act require companies to incorporate emails into their business processes. The US laws have been the subject of much recent debate in Europe too, and similar acts are currently being elaborated here too.

3.2 To Whom Do the Laws Apply?

All fiscally liable companies that produce, process or digitally transmit fiscally relevant documents by computer must observe the accounting and archiving laws.

3.3 What Are the Consequences of Breaking the Law?

Breaking these laws can result in costly legal proceedings, punitive fines running to millions of euros, third-party claims and, last but not least, considerable loss of reputation. The person responsible can even be handed jail sentences. On the basis of the German Data Protection Act and similar laws of other European countries, private individuals can assert even greater claims if they have suffered loss or damage due to the incorrect or negligent use and preservation of their personal data. The onus of proof concerning whether or not the data was handled with due care and attention lies with the defendant, not the injured party. In order to avoid claims, therefore, data needs to be backed up and archived properly.

3.4 Legally Compliant Archiving

An important aspect of the data laws in virtually all countries concerns legally compliant archiving. An electronic archiving system is considered legally compliant if the solution meets the requirements set out in the Commercial Code with regard to the secure and orderly preservation of commercial documents, and complies with the preservation periods of 6 to 10 years.

Since 1.1.2002, for example, the Federal Ministry of Finances has required all companies in Germany to prepare their fiscally relevant data in computerised format for verification on request by a tax inspector.

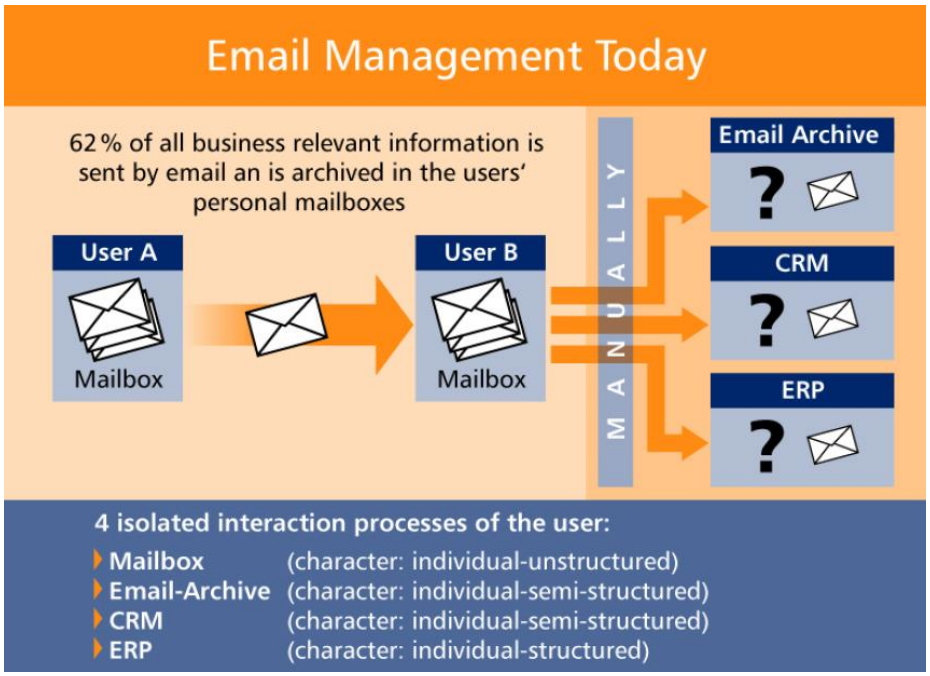
According to the law, tax inspectors must be given direct access to fiscally relevant, digitally generated corporate data, and this in addition to the option of inspecting all records, books and other commercial documents (preservation period of 10 years). Since 2005, fiscally relevant data must be formally correct during a digital audit, i.e. the principles for verifying computerised accounting systems in the context of external audits must be met. If the breach is repeated, sanctions such as estimation of the tax base or fines may be imposed. Several surveys suggest that only 10% of German companies meet these requirements. Most companies either completely ignore this obligation or comply only in part, with inevitable consequences in the event of a digital audit.

Of this 10%, many focus solely on the archiving of financial, investment and accounting data, with scant regard for the company's email correspondence. But data such as travel expense accounts, applications for leave, commissioning agreements, calculations, and contracts are frequently exchanged via email. According to the law, emails such as these are fiscally relevant documents. Together with their attachments, they must be archived and indexed without risk of subsequent tampering. Everybody knows the time and effort it takes to search for an email hidden away in the depths of a cluttered mailbox. Mailboxes occasionally need to be deleted in order to free up space and re-establish a certain order. In doing so, it is easy to delete a fiscally relevant item of information, which should really have been archived some time ago.

4 Optimising Business Processes

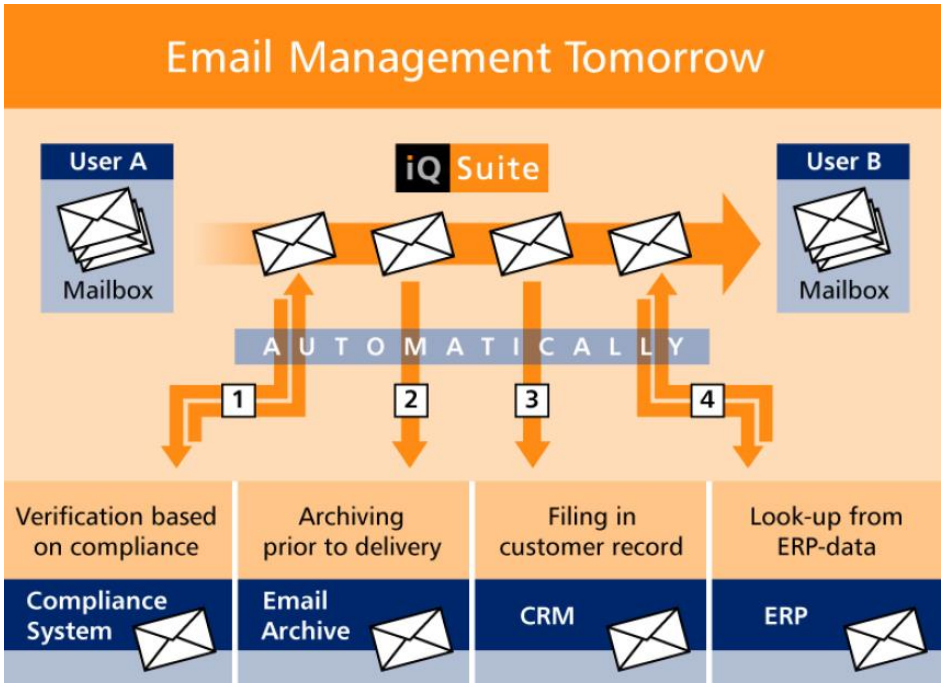
iQ.Suite Bridge plays a crucial role in the design of an email management system. Just as in conventional records management, the concept focuses on an email's entire lifecycle from cradle to grave. Designed by GBS Software, iQ.Suite is the toolbox for implementing this strategy in the workplace. iQ.Suite ensures that the moment an email is sent or received, it is organised in such a way that it can be retrieved, processed and stored by the company without risk during its entire lifecycle and without loss of context. All the verification, classification and filter processes that are run ultimately serve this one purpose.

Information Lifecycle Management (ILM) solutions do not come into play until the data is on the email clients ready for storage. Whether users have deliberately or accidentally modified the emails in the meantime, or even deleted them, is ignored. For this reason, proper and complete archiving of emails cannot be guaranteed with this type of solution. A company that relies solely on an ILM solution based on storage management risks legal sanctions if e.g. important data hidden away in emails cannot be produced at an audit.



With conventional ILM strategies, therefore, considerable potential for enhancing email usage in the workplace remains untapped. This is where email management enters the equation. Anyone who reduces the volume of messages received by installing spam software will automatically require less storage space. And anyone who sorts and classifies incoming emails and attachments straight away in accordance with flexibly configurable rules, before assigning them to individual business processes according to type and affiliation will be able to find those documents quicker when needed and archive them more efficiently. Email management is all about optimising email traffic so that staff can concentrate on the relevant business issues.

The graphic below shows how the solution works.



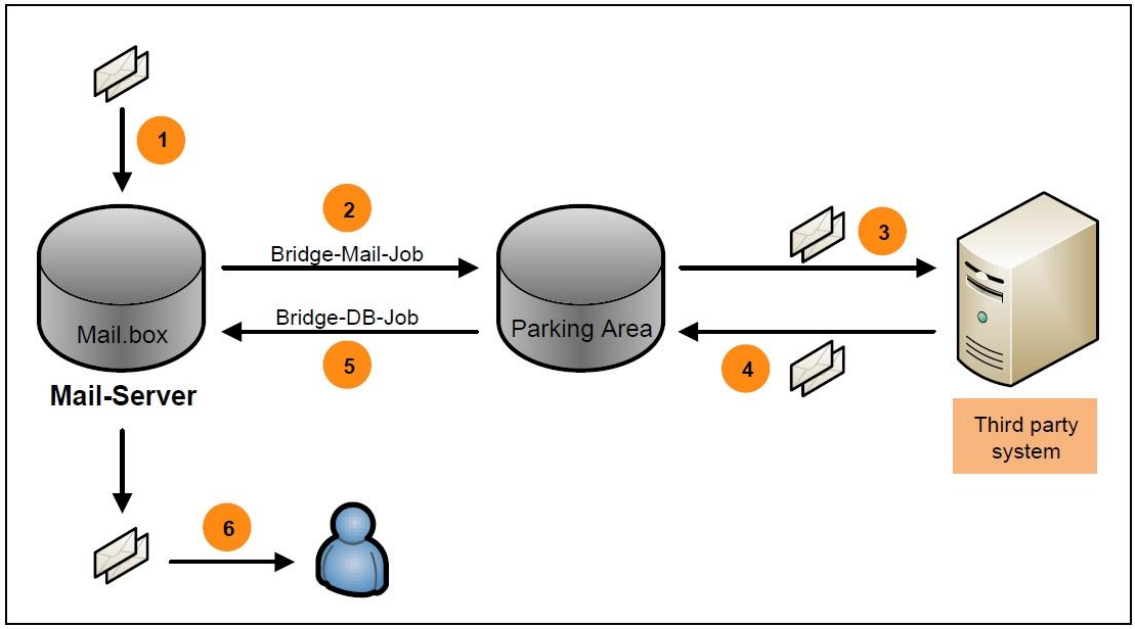
5 iQ.Suite Bridge – How It Works

iQ.Suite Bridge is the interface to external systems that helps users optimise their business processes while complying with the legal requirements.

With iQ.Suite Bridge, email data can be forwarded to external systems for further processing. iQ.Suite Bridge provides standard interfaces for connecting to

- Archiving systems – allowing entire emails to be picked up at the email server prior to delivery for centralised, tamper-proof transfer to an archiving system
- CRM systems (Customer Relationship Management) – allowing CRM systems to be connected to the email platform so that categorised customer information can be transferred automatically without individual employees having to spend time maintaining the CRM system
- ERP systems (Enterprise Resource Planning) – allowing information to be read from an email, structured, and then processed automatically by the ERP system
- Storage systems – allowing storage space on the messaging server to be reduced; with its integrated rule set, this type of connection has benefits over the journaling functions of messaging servers, e.g. during hierarchical storage management
- Compliance management systems – e.g. to introduce an audit system or have emails monitored by human operators. iQ.Suite Bridge parks emails until it gets the go-ahead from the compliance system to proceed with processing, then acts on the instructions received

The graphic below shows how iQ.Suite Bridge interacts with external systems.



1. Email is intercepted automatically and removed from the processing chain
2. Bridge parks the email in the parking area
3. External system accesses the email and processes it
4. External system places the processed data back in the parking area
5. Bridge takes the data from the parking area and continues processing
6. Email is delivered

iQ.Suite Bridge now provides interfaces for Saperion and IBM Commonstore in the field of archiving. By also linking up to iQ.Suite Store Pro, which provides additional functions, solutions from e.g. NetApp or Solitas can be integrated too.

The interface we developed with a partner based on a web service enables the email system to exchange data with SAP R/3 via iQ.Suite Bridge.

iQ.Suite Bridge's generic XML interface means that any number of additional archiving, CRM, ERP and compliance systems can be connected even if dedicated interfaces to them have not yet been developed.

6 Corporate Compliance

Besides statutory requirements, corporate compliance guidelines are the key motivation for organising and automating work processes. And while regulations governing e.g. staff and customer communication, storing data, workplace configuration and, last but not least, business correspondence are complied with almost as a matter of course, email guidelines are just as important for the well-being of the company.

Like all corporate guidelines, email guidelines are tailored to the individual needs of the company. Each industry sector will have its own priorities and these may vary from company to company. In the banking industry, for example, account information must remain inside the institution (banking confidentiality), while a research laboratory will want to make sure that its latest technical drawings do not find their way into the hands of the competitors via email. Anyone who has ever hit the Send button too soon knows how easy it is to pass on information to the wrong recipient by mistake.

The email business process should be organised such that the content and form of both inbound and outbound emails, including their attachments, comply with corporate guidelines. To this end, emails may have to be stopped prior to dispatch. iQ.Suite Trailer can ensure that outgoing emails comply with corporate design rules, while iQ.Suite Wall can classify the mails in advance before iQ.Suite Bridge forwards the filtered mails to a compliance system. The further processing of verified emails can take different forms. Emails cleared for delivery are dispatched, while problem emails are quarantined, forwarded to a third party, or simply deleted.

Email classification can be used in many different application areas. These include the automatic organisation and context-based storage of content, the creation of flexible delivery and distribution mechanisms, and the automatic indexing of archived emails.

iQ.Suite's comprehensive and extremely flexible rule set ensures that individual corporate guidelines are complied with.

7 Application Scenarios

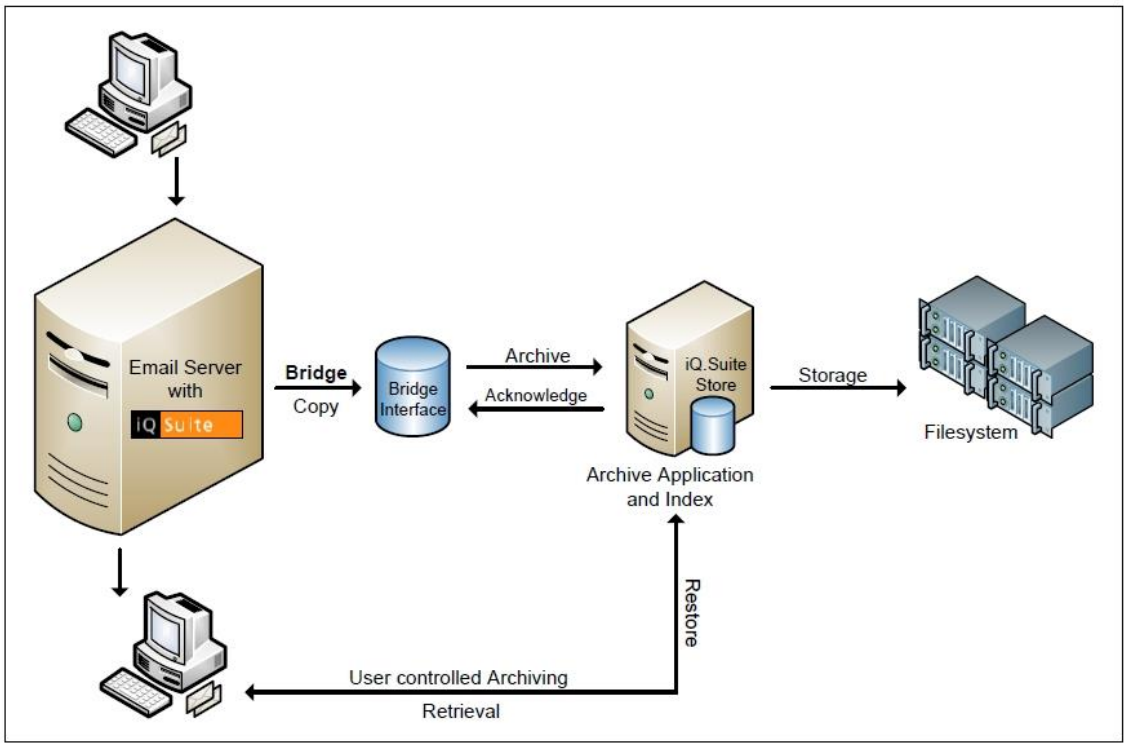
7.1 The Standard Solution With iQ.Suite Bridge and iQ.Suite Store Pro

Deployment in mid-sized to large companies:

You want your email storage solution to use the comprehensive functions and rule set of iQ.Suite in conjunction with an email archiving system such as iQ.Suite Store Pro. Both the retrieval and recovery of documents should be as transparent as possible, and be accessible by all employees.

Solution:

The seamless integration of iQ.Suite into the archiving system will ensure efficient and targeted email archiving. From now on, only business-critical emails will be archived, whether they are encrypted or not. If you are not yet using an archiving system, GROUP can offer you an integrated solution featuring iQ.Suite Bridge and iQ.Suite Store Pro. Duplicate archiving will be avoided and all irrelevant data filtered out. This will reduce the load on the overall archiving infrastructure.

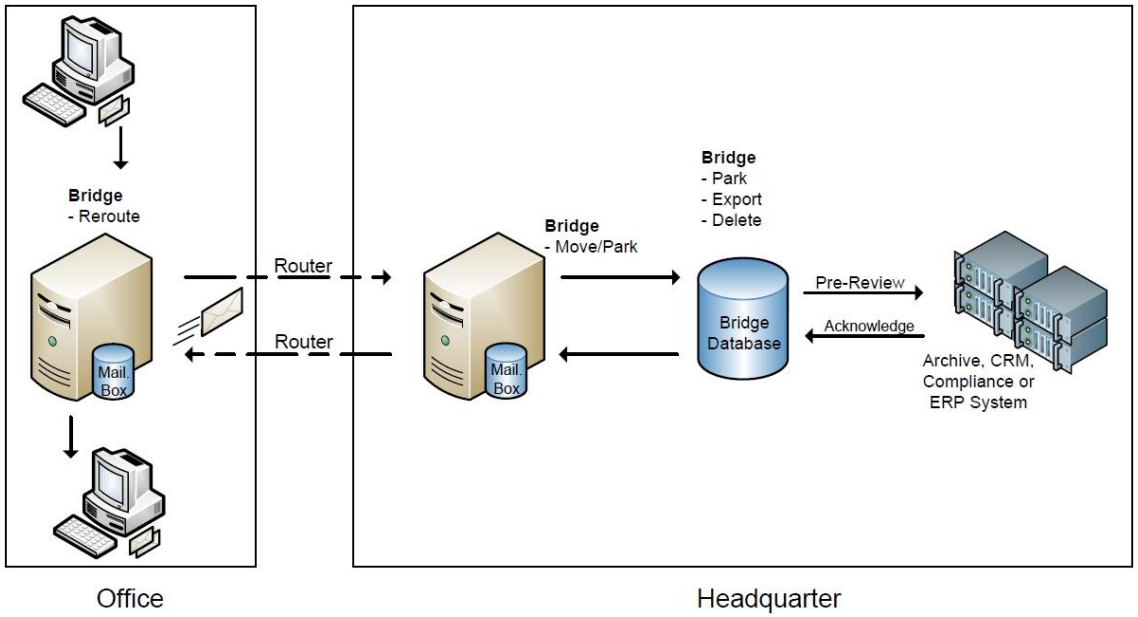


Deployment in group companies:

You need to comply with statutory provisions or corporate regulations governing emails and want to design a tailored, rules-based process. You want to connect your messaging platform with an existing compliance, CRM, ERP and/or archiving system.

Solution:

With iQ.Suite's highly flexible rule set and the iQ.Suite Bridge interface and compliance module, you can design an email process based on individual guidelines that can be finely tuned for pre-processing, filtering and classifying emails. Customising options allow you to craft a flexible, integrated solution which meets the diverse regulations down to the last detail.



8 Special Application Scenarios

8.1 Case Scenario - Archiving

8.1.1 Situation

A company operates a standard messaging platform and also has a commercial archiving solution in which client data and transactions are archived.

It is the company's objective to have its email communications securely archived, too. Previous approaches to email archiving focused solely on the end user. With this concept, the user decides which emails are archived and when. This kind of solution does not support full, audit-compliant archiving as it lacks a centralised and automated methodology. This is why iQ.Suite Bridge adopts the server- and rule-based approach, which allows emails to be archived in a proactive and time-controlled manner. Information is retrieved via the existing applications and components of the archive creator.

8.1.2 Proactive Archiving – A Sample Case

The aim is to identify archive-critical emails on the basis of their metadata and content, and then have them copied automatically and proactively – i.e. prior to delivery – to the archive system. In addition, the archived emails will be tagged with freely selectable status information (keywording) in order to simplify their further processing.

All relevant emails of the category "Finance" are to be archived for certain sender/recipient relationships. To this end, the sender and recipient addresses of inbound and outbound emails are extracted and the content category of the email or attachment determined (by CORE[1] in iQ.Suite Wall). A rule will be configured for iQ.Suite Bridge which will result in all emails of the content category "Finance" being processed further by iQ.Suite Bridge.

In accordance with the rule set, iQ.Suite Bridge will provide the archiving system with a copy of the email together with security and other information. The archiving system stores the copy of the email. Together with the email status, iQ.Suite Bridge is provided with other relevant information on the archived email in the form of an import data record. If additional information needs to be inserted into the email, the email will be parked during archiving. iQ.Suite Bridge then edits the response from the archiving system, modifies it where necessary, and inserts it into the still parked email as additional information. The following options are available:

- Status information on the progress of archiving in the message text
- GUID of the archived document
- Remove the original attachments and replace them with a link

The email is then forwarded with this data to the original recipient. If no information needs to be inserted into the email or changes made, standard "post-review" archiving will take place without the mail having to be parked at all.

8.1.3 Periodic Archiving – A Sample Case

The aim is to identify archive-critical emails on the basis of metadata and content, and then archive these mails periodically at certain times. The aim is to ensure that any changes and new documents stored by users directly in their mailboxes and databases are captured as well. In addition, the emails and documents to be archived will be tagged with freely selectable status information (keywording) in order to simplify their further processing.

All relevant emails of the category "Finance" are to be archived for certain sender/recipient relations. To this end, the sender and recipient addresses of inbound and outbound emails are extracted and the content category of the email or attachment determined (by CORE in iQ.Suite Wall). A rule will be configured for iQ.Suite Bridge such that all emails of the content category "Finance" being processed further by iQ.Suite Bridge. Via a user-specific configuration, the archiving system is provided with copies of the emails along with security and other information. The archiving system stores the copy of the email. Depending on the configuration, the original emails or mail attachments are deleted from

[1] **CORE is an email classification technology based on Support Vector Machines (SVM).**

the mailbox (or folder/database). Together with the email status, iQ.Suite Bridge is provided with other relevant information on the archived emails in the form of an import data record.

In time-controlled mode, static storage of emails means that they do not need to be parked. iQ.Suite Bridge edits the response from the archiving system and inserts it into the emails as additional information, or generates a separate status email.

The following options are available:

- Status information on the progress of archiving in the message text
- GUID of the archived document
- Remove the original attachments and replace them with a link
- Delivery of a status email

8.2 Case Scenario - CRM

8.2.1 Situation

A company operates a standard messaging platform and also has a commercial CRM solution (e.g. GEDYS IntraWare, SAP, etc.) in which client data and transactions are organised. It is the company's objective to have its email communications better integrated into the CRM processes, and to provide a complete customer file that includes selective email data. Up to now, email content had to be copied to the customer file manually. In future, this process is to be automated as far as possible, with inbound and outbound emails automatically forwarded to project files and CRM customers using a rules-based methodology.

8.2.2 Case

An inbound email is to be identified and a copy automatically stored in the customer file of the CRM system. Also, selected customer data has to be added to the email.

The sender and recipient addresses of inbound and outbound emails are extracted and the content category of the email or attachment determined (by CORE in iQ.Suite Wall).

A rule will be configured for iQ.Suite Bridge such that only emails of a certain content category will be processed further by iQ.Suite Bridge.

iQ.Suite Bridge generates a request for the CRM system in order to ascertain the customer file (CRM customer number, master data on the sender) on the basis of the sender address. Also, a copy of the email is sent to the CRM system. The CRM system determines the customer data and stores the copy of the email in the customer file. Together with the customer data, the data in the CRM system is forwarded to iQ.Suite Bridge in the form of an import data record.

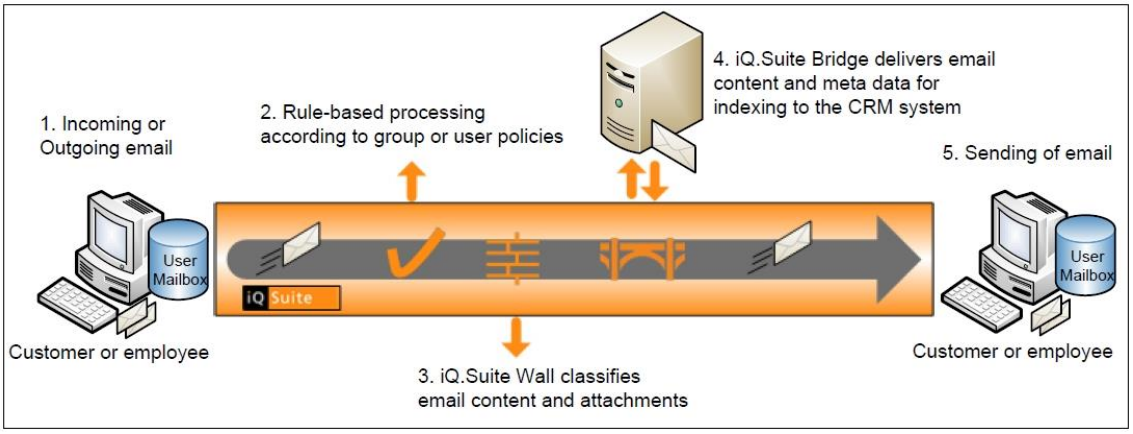
The email is parked for the duration of the request for data from the CRM system.

iQ.Suite Bridge edits the response from the CRM system and inserts it as additional information into the parked email.

Processing:

1. An employee of the defined group “Sales” receives an email.
2. The customer is identified via user-x@company.com and, possibly, other attributes.
3. The customer or project file in the CRM system is determined.
4. The content and any attachments of the email are forwarded to the CRM system using a rule-based methodology.
5. The data is stored in the electronic customer or project file.
6. The email classification attributes for creating the index and for automatic keywording are transferred.
7. The customer master data of the sender is added to the message text of the email.
8. A link to the CRM system is inserted in the message text as a footer or header.
9. As an option, a message detailing the process and the process number can be sent to the sender or the receiver.
10. The email is then forwarded with this data to the sales employee (original recipient). This can take place straight away, i.e. at the same time as processing, or afterwards.

Access to the CRM system is protected by the rule set.



8.2.3 Advantages

With iQ.Suite Bridge, the recipient obtains all the necessary contact data as well as a direct and qualified link to the customer file. Also, a copy of the email is sent to the CRM system.

The email can also be cleared for final assignment while it is in the CRM system. Analysing the inquiry more precisely can help identify incorrect assignment on the part of the account manager. For example, if the recipient of the email is no longer the correct contact partner for the customer in question, the email can be re-routed or forwarded to the correct account manager.

8.3 Case Scenario - ERP

8.3.1 Situation

A company operates a standard messaging platform and also has a commercial ERP solution (e.g. SAP, Navision, etc.) in which client data and financial transactions are organised. It is the company's objective to have its email communications better integrated into the ERP processes. Up to now, the office clerks in email communications have to work without important additional information from the ERP system. So far, they have had to research and retrieve this data manually from the ERP system. The aim in the future is for account managers to receive this information automatically with the email.

8.3.2 Case

An inbound email is to be identified, and selected customer data from the ERP system determined and added to the email in order to minimise office clerks time-consuming searches through the ERP system and allow them to respond faster to the email.

The sender and recipient addresses of inbound and outbound emails are extracted and the content category of the email or attachment will be determined (by CORE in iQ.Suite Wall). A rule will be configured for iQ.Suite Bridge such that only emails of a certain content category with recipients of a certain group will be processed further by iQ.Suite Bridge. iQ.Suite Bridge generates a request for the CRM system in order to determine the debtor master data (customer number, master data on the customer) on the basis of the sender address. Additional information such as turnover in the period, total open items, reminders, and credit rating is provided. The ERP system determines the queried data and makes it available to iQ.Suite Bridge in the form of an import data record.

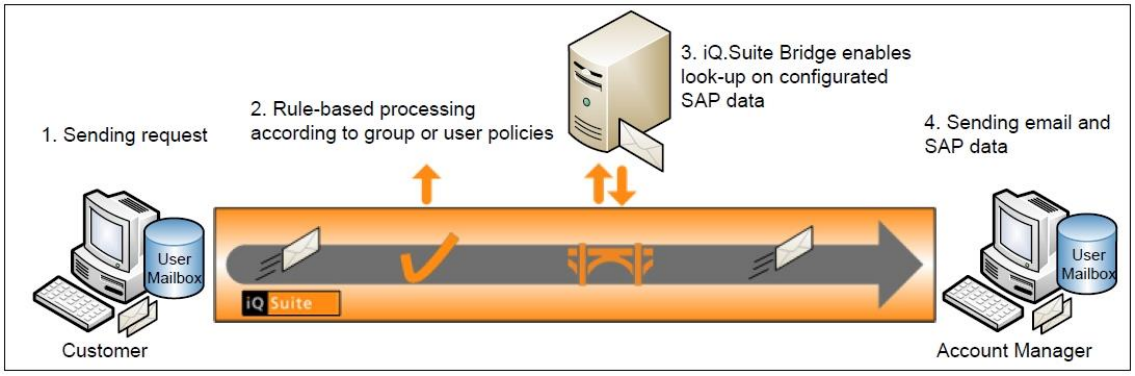
The email to recipients of the chosen group is parked for the duration of the request for data from the ERP system. The email is delivered to "other" recipients without parking, as iQ.Suite splits the recipients into "to be processed" and "not to be processed". iQ.Suite Bridge edits the response from the ERP system and inserts it as additional information into the parked email.

Processing:

1. A customer sends an email to sales@company.com or user-x@company.com.
2. The email is parked and the debtor ascertained via the sender address (employee@customer.com).
3. The defined SAP data is looked up subject to SAP access security rules:
   - Customer name and creditor number
   - Other master data:
     - Credit rating
     - Sum total or list of open items
     - Sum total or list of open orders/deliveries

4. The additional information is inserted in the email.
5. A link to the SAP system is inserted in the email.
6. The email is then delivered to the employees in sales.

Access to SAP is protected by SAP Security and by iQ.Suite's rule set.



8.3.3 Advantages

With iQ.Suite Bridge, only one recipient from the previously defined group obtains all the necessary debtor data and a direct and qualified link to the debtor file. Analysing the inquiry more precisely allows an email to be supplemented with additional graded information on debtors.

9 iQ.Suite Bridge at a Glance

- iQ.Suite Bridge is an interface to external systems
- As an integral part of the iQ.Suite, iQ.Suite Bridge features a fully modular architecture that has none of the shortfalls of a stand-alone solution
- iQ.Suite Bridge can be used on the IBM Domino and Microsoft Exchange email server systems, or on SMTP gateways
- iQ.Suite Bridge enables fully automatic archiving of inbound and outbound emails at a central location
- Emails are archived in such a way that they cannot be tampered with before delivery to the end-user
- iQ.Suite Bridge achieves seamless integration in leading archiving systems and ensures efficient email archiving
- iQ.Suite Bridge can be combined with iQ.Suite Store Pro to produce a seamless, centrally manageable email archiving solution
- External ERP, CRM and DMS systems can be linked in order to integrate emails in your business processes
- iQ.Suite Bridge can be linked to compliance systems for audits, and pre- and post-reviews
- A powerful yet flexible rule set supports the implementation of both statutory and corporate provisions and regulations
- Configurable converters allow the exchange of data between systems to be customised easily
- Scripting interface for pre- and post-editing of data
- Asynchronous methodology
- Complies with legal and corporate requirements
- Intelligent pre-classification is possible

About GBS

GROUP Business Software is a leading vendor of solutions and services in the fields of messaging security and workflow for the IBM and Microsoft collaboration platforms. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia.

Further information at www.gbs.com