



The iWay Security Exchange

Technology Brief

by Jake Freivald and Eric Greisdorf

Table of Contents

1	Executive Summary
3	Collaboration: The Imperative to Integrate
4	Collaboration and Integration Issues
4	Collaboration Issues in Government
9	Three Integration Methods
10	Data Consistency
12	Composite Application
13	Straight-Through Processing
17	The iWay Security Exchange
19	Security Integration Suite
20	Information Delivery Suite
22	Additional iWay Security Exchange Components
23	iWay Software and Information Builders
23	Federal Emergency Management Agency (FEMA)
23	U.S. Postal Service (UPS)
24	State of Pennsylvania
24	U.S. Department of Agriculture (USDA)
24	U.S. Department of Agriculture (USDA) – Rural Development
25	Contact Us for More Information

“If I were Tom Ridge, the first dollar I would spend would be on data integration.”

Sandy Berger
Former National Security Advisor
Federal Computer Week
October 18, 2001

Executive Summary

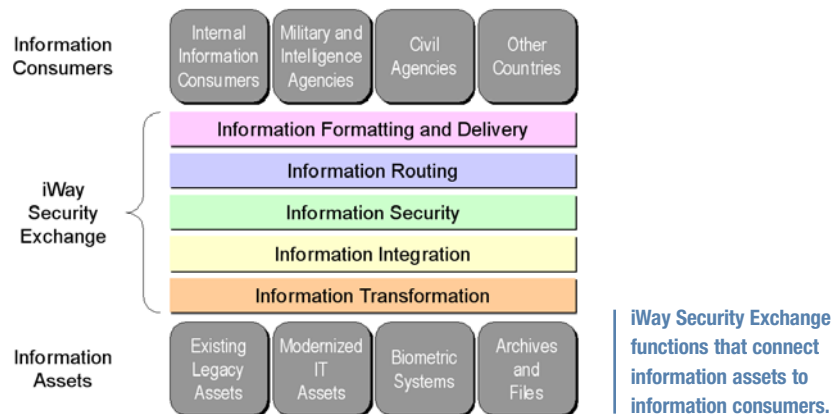
The need for integrated and collaborative security exchanges is as clear and immediate as today's headlines. Leaders of intelligence, law enforcement, and other agencies must determine the best way to exchange national security information in a rapid, secure, and reliable way – and to use major new budget appropriations that target this need.

Integration is the creation of a collaborative network of different information systems, agencies, and processes. For true inter-agency collaboration, any solution must help all the agencies' current and planned information systems act as a coherent unit.

For example, security organizations already have processes to monitor, track, and apprehend criminals and suspicious parties. These processes would be far more effective if they had immediate access to information from another agency, state, or even country.

Although conceptually simple, law enforcement and intelligence agencies struggle to solve this difficult policy and technology puzzle. Integration within a single organization is hard. Inter-agency integration can be orders of magnitude harder.

The iWay Security Exchange (iSE) uses integration technologies from iWay Software and IBM to create collaborative frameworks for exchanging existing security information across department, agency, and even national boundaries.



This brief discusses the iSE in the context of integration challenges for homeland defense and national security, such as preserving agency independence, maintaining privacy and security safeguards, streamlining the creation of collaborative processes, utilizing existing IT assets, delivering information, and handling new technologies like biometrics and face recognition.

The advantages and disadvantages of the three major integration approaches, as defined by Gartner Group, are also covered:

- **Data consistency** – creating a new central information repository, often called a “data warehouse,” that is periodically refreshed with data from a variety of information systems.
- **Composite applications** – building new applications that transparently connect existing applications to each other in real time to fulfill a task.
- **Straight-through processing** – centrally managing a process through a series of clearly defined steps, each owned by the most appropriate organization. This is the most important integration approach for managing collaboration across agencies.

We conclude with a discussion of iSE technologies and tools, as well as award-winning security solutions already crafted by Information Builders and iWay Software.

Collaboration: The Imperative to Integrate

What lessons have we learned from the terrible events of 9/11? Certainly we now possess a heightened awareness of the need for an integrated, collaborative approach to threat management: generating actionable information from new or existing sources and getting it into the hands of the people who need it in good time.

The need for a high level of collaboration is absolute and as close as headline stories like these:

- 5,000 shipping containers enter New Jersey every day, but there are only enough Customs Service resources to search 500 of them. In Southern California, the situation is worse: 7,500 containers shipped but only 750 inspected. **How can information be developed to more accurately target searches based on relationships that crews, nations of origin, and cargo have with terrorist organizations such as Al Qaeda?**
- 9/11 terrorists had been stopped several times in different locales by local law enforcement. Nine of them were stopped at the airline gate because of profiling or ID problems, yet were ultimately allowed to board. **How can known patterns be used to help identify suspicious people?**
- Several 9/11 suspects obtained drivers licenses, HAZMAT licenses, gun permits, and flight training while information about them was being passed from the CIA to the INS to the FBI. **How can information latency be reduced?**
- Intelligence shows that Al Qaeda figures have plans for our nuclear power plants and water treatment facilities. **How can loiterers, trespassers, and suspicious activities at such sites be quickly and completely checked out via wireless devices?**
- INS reports that 30,000 immigrants have ignored deportation orders. Approximately 6,000 from countries with strong Al Qaeda support have all gone underground. **How do we find them?**
- Recent budget increases are intended to improve border patrols by hiring more agents. But systems integration is an absolute necessity, too. **How can integration dollars be spent where they will have the most impact?**

The role of collaboration in solving these problems cannot be underestimated. None of these issues can be adequately addressed unless people, agencies, and information systems work together in an integrated fashion.

Collaboration and Integration Issues

Traditionally, Federal agencies such as the INS, CIA, and FBI have each concentrated on providing the best information possible within their own domains. Indeed, there are rules and laws governing the boundaries of each of these agencies, primarily to protect the civil rights, liberties, and privacy of American citizens.

Prior to September 11, it was believed that the processes being used for information exchange were sufficient to protect American citizens from harmful attacks while also protecting the civil liberties that Americans are accustomed to.

Since September 11, various agencies have made a number of changes to their processes, including:

- An increase in the number of field agents and personnel
- Stricter visa requirements
- More stringent security for travelers
- Increased patrols and a heightened level of readiness
- Public awareness campaigns

To be effective, these changes must be accompanied by increased inter-agency collaboration.

Collaboration Issues in Government

Many government organizations struggle with collaboration because of a variety of policy and “Washington culture” issues. Technology alone cannot solve political and policy problems, but the iWay Security Exchange can provide a partial solution in many cases, or at least ensure that technology is not the major stumbling block.

One can’t hope to address every issue in a single paper, but some leap to the forefront.

Agency Independence

Key points:

- Agencies must maintain their own processes
- Agencies must control data for which they are responsible
- Agencies must deal with their current infrastructure realities

No agency has only one task. Intelligence agencies, for example, must collect intelligence on foreign nationals, protect their sources through compartmentalization and sanitization, and preserve citizens’ rights by keeping citizen and foreign national data separate. An agency will – and should – balk when collaboration requirements appear to threaten its ability to function effectively.

There is also no clear mandate on liability for the use of information. Agencies that are required to protect the information that they use must also share it with organizations that may have different standards, requirements, and legal mandates to follow. If organization A releases information to the public based on protected intelligence received from organization B, has organization B failed in its duty to protect that information?

Finally, each agency must have the freedom to deal with its current infrastructure realities in the way that would most benefit its mission. Computing platforms, databases, skill sets, and processes will not change overnight. It would be a tremendous risk – not to mention a colossal expenditure of money and time – to rip out and replace all of the information systems that currently run operations and house critical information. Agencies must be able to leverage what they currently have while still engaging external organizations.

Security and Privacy Safeguards

Key points:

- Collaborating systems must respect compartmentalization, sanitization, and the need to know
- Agencies must control privacy without crippling information-sharing processes
- Authentication of need and delivery of information must be fully auditable

Collaboration processes must respect the need for compartmentalization, sanitization, and discrimination based on the need to know. The intelligence community maintains security in part by breaking intelligence into compartments based on the source of the information. Only by “sanitizing” intelligence – removing all indications of the way the intelligence was gathered – can information be decompartmented. Moreover, even fully cleared personnel will be denied information if they don’t have a need to know it. These rules are crucial; only by following these safeguards can the intelligence communities ensure that their sources will continue to provide exploitable information.

Law enforcement and social services agencies are similarly concerned with privacy. For example, law enforcement must prove that private records are likely to contain information about criminal activity before a warrant can be issued to seize them. Agencies must be able to show that they behaved correctly during collaboration activities, so that privacy concerns can be addressed without crippling information-sharing processes.

A collaboration infrastructure must support these requirements and more. A request for private information must be rejected if there is no basis for it. And when a request for private information is granted, it must travel across a secure network, arriving once and only once, with an audit trail if necessary to ensure that legal requirements have been met.

Intelligent Streamlining of the Collaboration Process

Key points:

- Internal processes must be integrated to support external ones
- Repetitive tasks should be automated by computers
- People should be reserved for tasks where judgment is important

Assume for a moment that several organizations have streamlined their collaboration process through Web interfaces, e-mail messages, wireless devices, and messaging systems, so that now they can support 1,000 requests for information per day from virtually any authorized requestor. That effort has been wasted if the internal processes of the organizations can only support three requests per day.

This is not a new issue, or a minor one. We can learn from several public failures in the private sector during the dot-com craze: companies built Web sites that allowed thousands of people to order goods online, but the orders were processed by hand and couldn't keep up with demand. The result was late shipments, dissatisfied customers, and bad press. These sites only became successful after the internal processes had been automated to handle the additional workload.

Computers perform repetitive tasks better than people do, causing fewer errors and providing greater throughput for many tasks. They can flag an expired visa, provide the date of a handgun sale, or crosscheck a criminal database with little or no human intervention. Computers should free people to focus on tasks that need judgment, like improving processes and resolving ambiguous or contradictory policies. People are too important to leave to mundane tasks.

Modernization Programs and Use of Existing Mission-Critical Assets

Key points:

- Integration technologies must not interfere with modernization efforts
- Integration is preferable in most cases to hurriedly rewriting legacy applications
- Integration reduces redundancy, security issues, time to collaboration, and cost

Nearly every Federal agency has a modernization program in place and scheduled for completion within 5 to 10 years. The drive to collaborate makes the move to more modern, open systems even more appealing than before – but collaboration can't wait a decade.

One option is to replace existing systems on a more rapid timetable. This approach is both risky and costly, however, and effective mission-critical systems should not be torn out and replaced with untested applications without a serious analysis of risk and reward. Also, since no agency can transform its infrastructure overnight, some level of legacy integration will always remain. Another option is to duplicate some of the data and functionality from a legacy application in a new application. While this solves the basic problem, it creates other issues through duplicate maintenance, data consistency problems, and latency.

Rather than avoid the legacy integration issue, agencies should strive to incorporate legacy databases, external data feeds, and other information assets into its overall solution. Benefits of this approach include faster delivery of the complete solution, a reduction in the overall cost of the solution, decreased data redundancy, and fewer security touch points. As modernization programs continue, these older applications can be phased out in a logical fashion, according to priorities of the time.

Information Delivery

Key points:

- Integration must support on-demand inquiries (“pull”) and alert-based (“push”) information delivery
- Information delivery is best if it can go to devices that users are already comfortable with

Information is only useful if it is delivered in a consistent, reliable, secure, and flexible way. To be effective, collaborative applications must push critical alerts to the people who need them, on any device they use for communication. Common approaches, like e-mail or Web browsers, are best if the information is unclassified or the delivery path can be secured. At the same time, field agents and agency workers must be able to pull information on demand to corroborate intelligence, make informed decisions, and perform basic research.

The information delivery platform must work with all of the collaborating information systems inside and outside of an agency, or it will only be able to show a fraction of the complete picture.

Solution Flexibility

Key points:

- Integration solutions should minimize custom integration code to maximize flexibility
- Applications and external agencies should be “black boxes” to make additions and changes easier

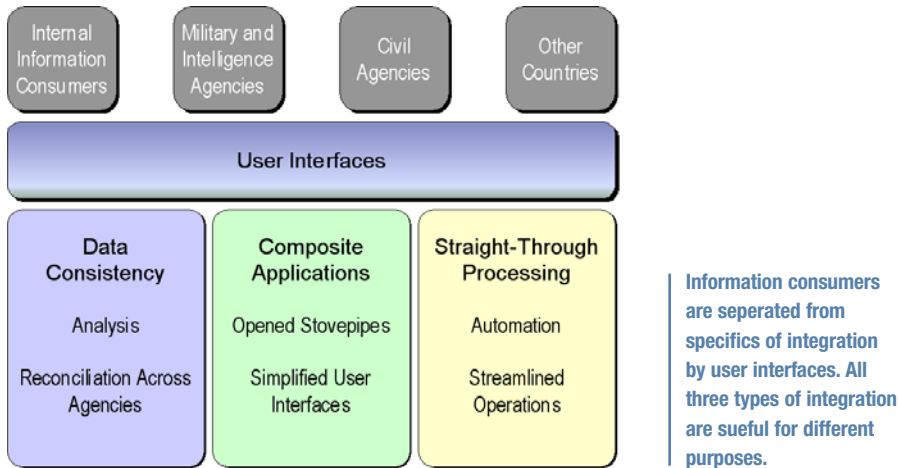
Many integration solutions impose restrictions on future change, instead of allowing greater change in the future. This is especially true for solutions that involve legacy systems or a lot of custom integration programming.

A collaboration platform should increase flexibility by reducing the workload on programmers, thereby making changes easier. Other applications should appear to be “black boxes,” components that plug and play without requiring programmers to understand their internal functions. Even other agencies should be simple to integrate, with common data exchange formats that can be easily modified and mapped to each other. For example, if a user manually inputs a name in order to get a visa status, it should be simple to add a biometric system that can provide the same information from a fingerprint. At the same time, it should be simple to add an entry point for another agency to provide the name and get back appropriate information.

Three Integration Methods

Integration technologies play a tremendous role in creating a resilient foundation for collaboration. Integration specialists coined terms that include middleware, enterprise application integration (EAI), messaging and queuing (MQ), and extraction, transformation, and load (ETL) to describe the types of integration technologies that can be used to form collaborative environments.

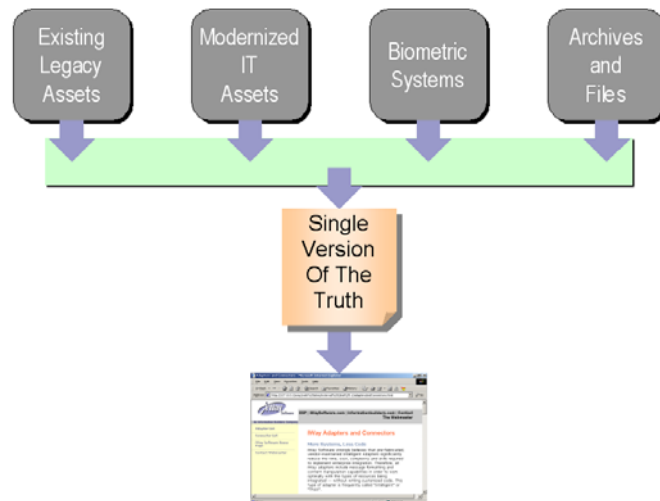
Rather than discuss integration in terms of technologies, the Gartner Group classifies three basic types of integration based on the functions that they serve: data consistency, composite applications, and straight-through processing. None of these is inherently superior to the others. Each solves a different type of problem and has different trade-offs.



iWay Software is unique in the industry for providing all of the necessary technology to manage all three integration types. The iWay Security Exchange centers on straight-through processing, but may have elements of data consistency and composite applications for a specific implementation.

Data Consistency

Data consistency involves making copies of sets of data on a scheduled basis to ensure that data in one application is reflected correctly in another. Data consistency can be considered analogous to bulk postal mail. With bulk postal mail, everything is sorted at the post office, organized neatly, and then delivered once per day at most locations. With data consistency, all data is extracted by the ETL tool or program, organized, aggregated, and delivered to the target database at some scheduled interval.



Data consistency reconciles information on a fixed schedule to create a “single version of the truth.” Data is typically only transferred one way.

Data warehouses, data marts, operational data stores, and reporting databases are all forms of data consistency that are useful in a collaborative process. Other uses include application reconciliation and batch processing. Data consistency is the most common form of integration, comprising about 80 percent of all the integration done today.

Advantages

“Single version of the truth.” Data from multiple databases can be correlated before loading into a data warehouse or data mart, reconciling apparent differences among reports.

Optimized for performance. Operational systems are optimized for transaction performance, so complex reports and analysis typically don’t perform well. As data is moved from operational systems, it can be staged in a way that makes common types of reports and queries more efficient.

Protect online resources. Not only do reports run slowly on operational systems, they also consume resources that could otherwise be used to process transactions. By moving data when the operational systems are not under a heavy workload, data consistency ensures that there is enough capacity to process transactions.

Easy to query. As data is loaded into a data warehouse or data mart, obscure structures and hierarchies can be removed, leaving users with a spreadsheet-like table that is easy for them to understand and query.

Centralized data administration and security. Because all of the information is ultimately placed in a single database, one team can manage all security and administration for the data.

Disadvantages

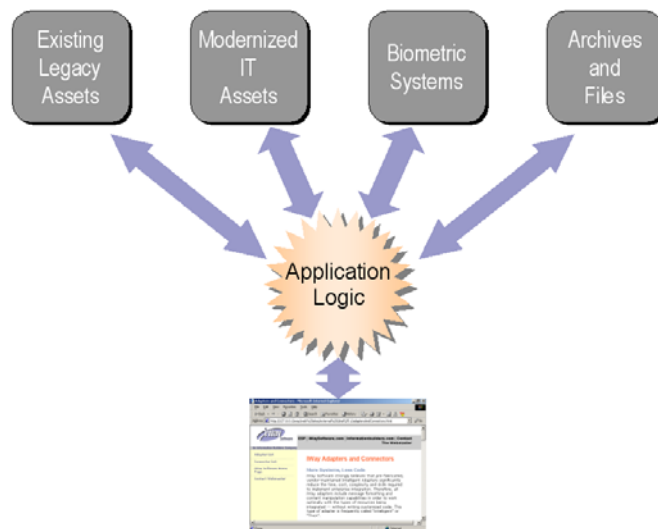
Latency. Because the data is moved on a scheduled basis, applications that require real-time information should not rely solely on data consistency.

Data ownership and accountability. Because data is no longer managed by the application that originated it, either the data must be sanitized or the data administration team must duplicate security information from the source application. In addition, accountability becomes cloudy as ownership of the data changes hands.

Legal and political issues. Data consistency is not acceptable for applications that require information about foreign nationals and American citizens. The Patriot Act forbids the merging of these two types of data into a single database.

Composite Applications

Composite applications connect information systems together, creating one application out of many – an application that is a combination of many other applications. Data does not have to be written to a separate database; it can be managed by the applications that created it. Composite applications usually function in real time, and frequently use a Web browser as the user interface.



Composite applications reuse existing logic in new, typically real-time, applications.

Composite applications can be considered analogous to the telephone. With the telephone, two people (or fax machines, modems, etc.) communicate in real time with immediate feedback. If one person, fax, or modem goes off-line, the communication cannot continue effectively. With composite applications, several underlying applications communicate in real time with the composite application. If one underlying application goes off-line, the application ceases to function normally and must provide some sort of backup.

Advantages

Real-time integration. Because composite applications use other applications as building blocks, the information in the composite application is always the same as the data in the application of record.

Reuse of validation and business logic. If the composite application accesses the underlying applications directly, it can take advantage of validation logic and business logic that already exists. This reduces overall development timelines and maintenance costs.

Support for Patriot Act. Since data doesn't have to be written physically to a database, citizen and non-citizen data can be merged in real time and used for intelligence, tracking, or threat identification.

Better ownership, security, and compartmentalization. Since the underlying applications are still under the control of the organizations that own them, the information that gets used is still under their control as well. In situations where compartmentalization is an issue, composite applications can decentralize control to the people who need it.

Disadvantages

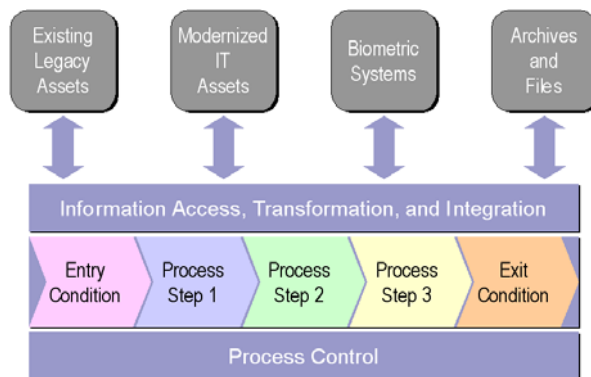
No more "single version of the truth." Real-time processing does not provide sufficient time to reconcile significant semantic differences among systems.

Stringent availability requirements. Real-time composite applications require all underlying systems to be online and ready to work. If a system goes down or is under a heavy workload, the composite applications may time-out or malfunction.

Contention. The additional strain of a real-time composite application on an operational system may cause it to suffer diminished performance for its primary task.

Straight-Through Processing

Straight-through processing involves the automation of step-by-step processes, using a central "integration broker" that uses messages to coordinate the activities of many different applications. Messages are frequently not acted upon in real time, but are acted upon "as soon as reasonably possible" or in "near-real time." This improves the overall stability of the system, because not all systems need to be up simultaneously in order for the process to work.



Straight-through processing integrates information as it is needed as part of a step-by-step process.

Straight-through processing can be considered analogous to e-mail. With e-mail, the sender and the receiver do not have to be online simultaneously. The sender sends his e-mail to a central server, which then waits until the receiver is online and then immediately delivers it. With straight-through processing, events are controlled by the integration broker, which manages system interactions even if some applications are down or sluggish because of a heavy workload.

Advantages

Robust processing. Near-real time processes handle application failures, sluggish response times, and other issues easily because they do not require real-time interactions and feedback. Integration brokers usually provide assured delivery (also called “guaranteed delivery”) and built-in recovery.

Data ownership. Because each application maintains its own security and is managed by its own team, compartmentalization and data ownership is improved. The application owners can determine how to respond to messages, instead of exposing business logic in ways that they will not be able to control fully.

Agency independence. In the same way that data ownership improves, agency independence improves because each agency or organization retains its own internal process as it determines how to respond to messages.

Security. Better data ownership and agency independence vastly simplify security requirements, which devolve upon the data and process owners.

Compliance with legal requirements. Messages do not have to be physically written to databases, which allows them to contain foreign national and citizen data simultaneously.

Simple to change an integration point. Since the processes are loosely integrated through the sending of messages, it is not difficult to send an additional message to incorporate a new agency, division, or application.

Disadvantages

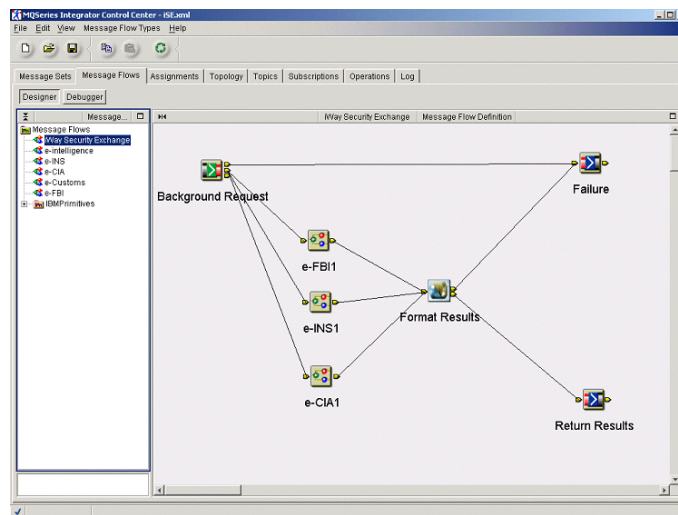
Can be complex. The messaging, integration broker, and adapter infrastructure can be complex. One of the iWay Security Exchange’s key differentiators is the simplification of straight-through processing implementations.

Can be expensive. The connections into legacy systems can be expensive. The iWay Security Exchange distinguishes itself with a toolset that keeps this type of solution very cost-effective.

Example

Because straight-through processing is so important to robust information exchange, the next few paragraphs and images show an example of straight-through processing and its implementation using IBM's WebSphere MQ Integrator and the iWay Plug-in Suite for WebSphere MQ Integrator.

Assume that an intelligence agency receives suspicious information about a particular person. That agency can submit a request for additional information to other agencies by formatting a message that contains the person's name and putting it into a message flow in WebSphere MQ Integrator. In the screen captured below, the agency is requesting information from the FBI, the INS, and the CIA.

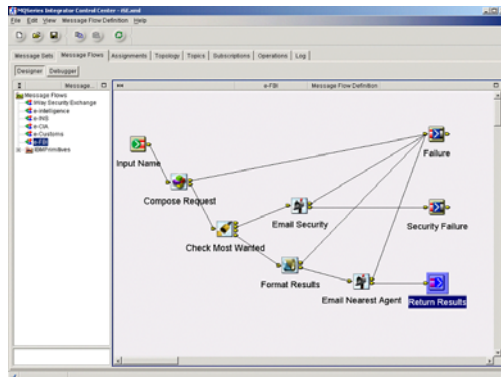


An agency is requesting information from an FBI, the INS, and the CIA by sending messages to those organizations.

As the information is returned from each of those agencies, it is reformatted, compared to tracking criteria, and sent as a failure (if there was an error in processing) or a success (in which case it returns results to the user).

Note that the requesting agency has no information about the internal processes of the FBI, INS, or CIA. It simply sends messages to which those agencies respond.

Changing our viewpoint for a moment, we can see what happens inside the FBI.

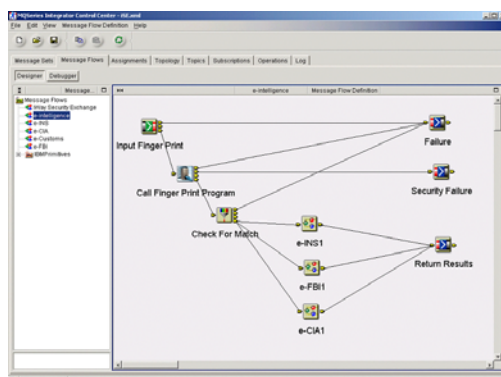


The FBI's internal process, shown here, is unknown to the requesting agency.

The FBI's process first uses iWay's XML Transformation Engine to select the name from the incoming message and apply a transformation that puts it in a request document for the Most Wanted database.

Based on the information returned, the FBI can deny the operation altogether, flag a security failure, or notify relevant agents that the suspect is in their territory. The security error will result in the calling agent not receiving the requested information. As long as there is no security failure, the calling agency receives the information needed. Note that collaboration in this case benefits both organizations, because the FBI was able to trigger activity based on the name entering its system.

Finally, suppose that the original intelligence agency now wants to include a recently installed fingerprint system as part of their detection process. They simply add a new node to the message flow that accepts a graphical view of a fingerprint, submits it to the new fingerprint system, receives a name in return, and then continues operations as before. Minimal changes are required for this process, and absolutely no changes are necessary for the INS, FBI, or CIA.

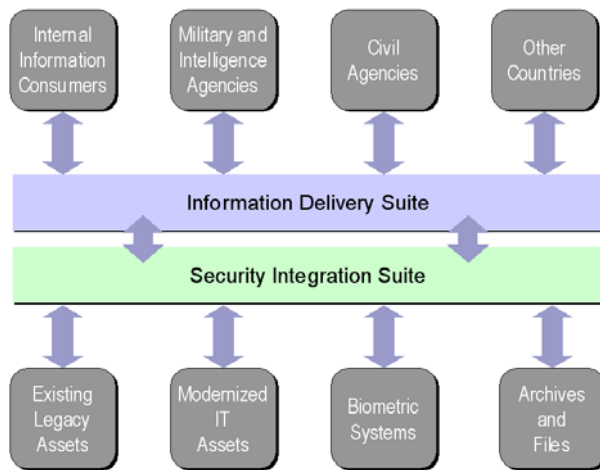


Extensibility is demonstrated by the addition of biometrics – a fingerprint system – with minimal additional effort locally and no changes at all to the INS, FBI, or CIA.

The iWay Security Exchange

The iWay Security Exchange, or iSE, contains all of the iWay Software and IBM tools necessary to integrate applications using data consistency, composite application, or straight-through processing methods.

Two major software suites make up the iSE: the **Security Integration Suite** and the **Information Delivery Suite**. The Security Integration Suite is designed to make it easy to integrate information systems for transactional composite applications and straight-through processing applications. The Information Delivery Suite emphasizes composite applications that focus on reporting and other forms of information delivery. Data consistency requirements can be addressed through the optional Warehouse Deployment Option, which can be added onto either the Security Integration Suite or the Information Delivery Suite.



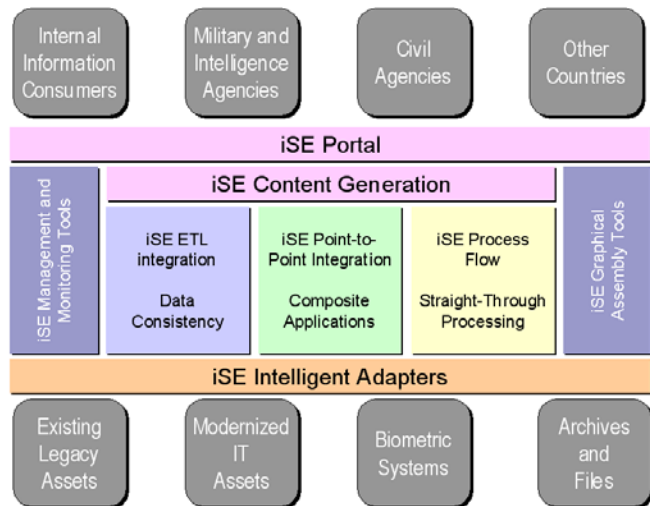
The Security Integration Suite and Information Delivery Suite work hand-in-glove to integrate and deliver information across disparate systems and different organizations.

iSE capability highlights include:

- Secure, reliable information exchange within a single agency
- Secure, reliable information exchange among multiple agencies
- Agency independence: participating agencies each maintain their own processes
- Maximum utilization of existing technology assets with minimum custom integration code
- Flexibility to switch from aging legacy systems to modernized systems with minimal disruption
- Ability to add or remove external agencies from processes with minimal disruption
- Ability to “pull” information from technology assets on demand
- Ability to “push” alerts from technology assets to e-mail and mobile devices
- Automation and auditability of key collaboration processes

iSE technology highlights include:

- Assured message delivery through IBM's WebSphere MQ (formerly MQSeries) message-oriented middleware
- Intelligent message integration and routing through IBM's WebSphere MQ Integrator (formerly MQSeries Integrator) technologies
- Sophisticated transformation technology through iWay Software's XML Transformation Engine
- Highly scalable Java™ engine for reporting and composite applications through IBM's WebSphere Application Server
- Information delivery to Web browsers, wireless devices, e-mail, and more – without plug-ins or complex deployments – through Information Builders' WebFOCUS
- Comprehensive information access and connectivity across the entire solution through iWay Software's Intelligent Adapter Suite
- Simplified integration assembly and custom-code avoidance through iWay Software's graphical integration tools and plug-ins



iSE includes technologies for achieving any of Gartner Group's three key integration scenarios, plus content generation and portal and data management tools that work across the entire solution.

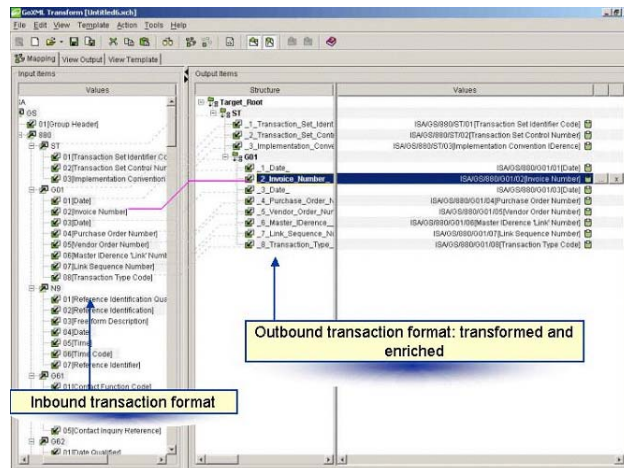
Security Integration Suite

The Security Integration Suite includes the iSE components for both composite applications and straight-through processing. The composite applications components are primarily directed toward transactional integration.

Composite Applications Components

The components for composite applications are primarily directed toward real-time transactional integration and include:

- A real-time integration engine for documents, including XML and non-XML formats, and a wide variety of applications and data sources. This component, which is based on iWay's XML Transformation Engine and Intelligent Adapter Suite, is also reusable for straight-through processing with IBM WebSphere MQ Integrator.
- An application server designed to host Java™-based composite applications. This is based on IBM's WebSphere Application Server and iWay's Enterprise Connector for Java™ Technologies.
- A resource analyzer that determines which requests are most common and resource intensive, based on iWay Resource Analyzer.
- A resource governor that lets administrators define what types of queries they want to allow, and terminates any that do not fit that profile, based on iWay Resource Governor.

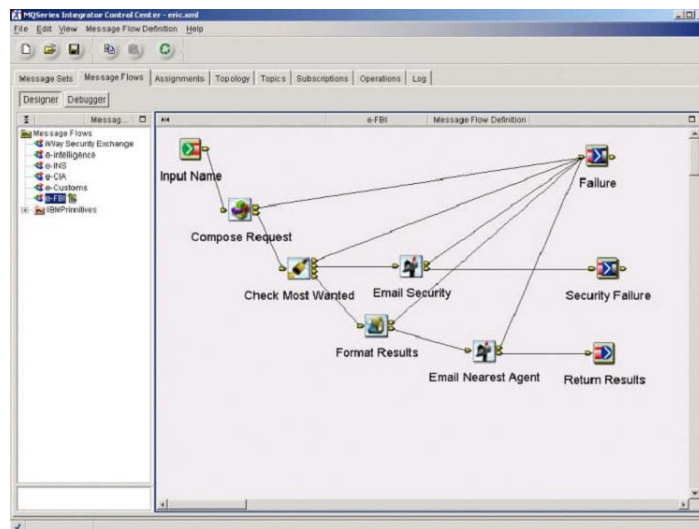


iSE makes it easy to map information from a set of sources to a set of targets, regardless of types.

Straight-Through Processing Components

The components for straight-through processing manage near-real time step-by-step processes and include:

- An integration broker, based on IBM WebSphere MQ Integrator, that provides intelligent message routing and delivery.
- A formatting and transformation engine, based on the iWay XML Transformation Engine.
- More than 200 intelligent adapters that provide access to application data and electronic message formats.
- Graphical plug-ins that link WebSphere MQ Integrator to the iWay toolset.



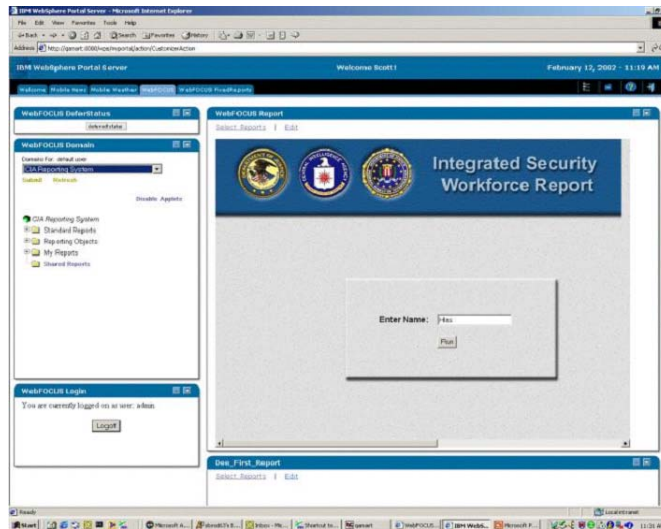
A process flow within iSE's straight-through processing tool. Each box on the screen is an application or agency accessed within the flow.

Information Delivery Suite

Information Delivery and Portal Capabilities

Because every agency needs a combination of real-time and historical data, iSE's Information Delivery Suite provides the ability to report off a variety of information sources – more than 200 in all, including live applications and databases, or even information as it flows through an iSE straight-through process. This capability, based on iWay's Intelligent Adapters and WebFOCUS (from iWay's parent company, Information Builders), makes iSE absolutely unique in the integration solution marketplace.

Information relevant to security can be obtained by a composite application in real time, through data staged in a relational database, or a combination of the two. No other solution provides this capability to frontline agents and knowledge workers.



iSE Integrated Reporting and portal option.

Components of the Information Delivery Suite

- Open portal services that enable you to deliver and integrate security information within third-party portals. Reports can include information from databases, messages, transactions, and applications.
- A report distribution engine that provides powerful and flexible scheduling and broadcasting of reports. Reports can be delivered in virtually any format anytime – including as alerts.
- A mobile reporting server which delivers Web-based reports and information from data sources and applications directly to a wide variety of mobile computing devices. The server supports data capture and updating of back-end data sources from handheld devices in real time, a feature that is unique in the industry.
- iWay Resource Analyzer, which provides reports on who accessed which information systems at what time and the types of queries they ran. This valuable tool is essential for both resource and systems security management.
- iWay Resource Governor, which lets administrators define what types of queries they will allow and to terminate any queries that do not fit a certain profile.

In addition, the Information Delivery Suite supports phonetic matching, a capability that is critical when working with global security issues. With phonetic matching, linguistic anomalies and spelling errors won't interfere with your search for information about foreign or domestic threats.

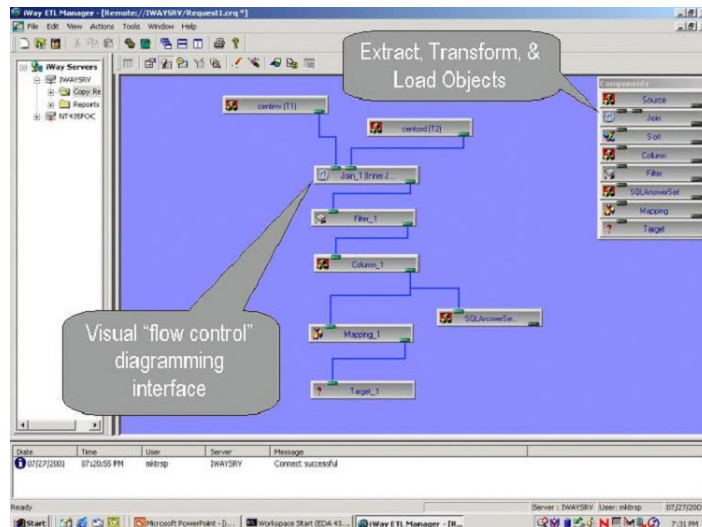
Additional iWay Security Exchange Components

Additional components are available in the iSE framework for:

- Data consistency (data warehousing, data marts, and so on)
- Data monitoring, profiling, and quality assurance
- Immediate linking into agencies such as the National Crime Information Center (NCIC)

The iSE Data Warehousing Option manages data consistency requirements and consists of the following components:

- An extraction, transformation, and load (ETL) tool called iWay ETL Manager



Extraction, transformation, and load (ETL) tool user interface.

- iWay Metadata Manager tool provides impact analysis and “where used” information for source and target information sources

The iWay metadata management tool and adapters are completely compatible with WebFOCUS for information delivery.

iWay Software and Information Builders

Headquartered in New York City, Information Builders has been providing commercially available, off-the-shelf software to federal, state, and local governments since 1975. iWay Software is an integration-oriented subsidiary.

Information Builders and iWay Software enjoy considerable trust due to long-standing success in federal, state, and local government IT establishments. Here are just a few examples.

Federal Emergency Management Agency (FEMA)

The staff at FEMA coordinates disaster response when the President declares a state of emergency. When the disaster involves flooding, FEMA's National Flood Insurance Program (NFIP) manages information flow. A system developed using Information Builders' technology enabled the NFIP to move from a slow, paper reporting system – where individual reports could be up to 18 inches thick – to a Web-based reporting system that allows staff to analyze claims by area, dollar volume, and insurance provider.

First used during Tropical Storm Allison, which killed 34 people and destroyed 16,000 homes, the application was deployed to local FEMA staff using portable computers with wireless Internet connections. In addition to providing critical data in a timely manner, the system was implemented using existing databases and infrastructure, saving an estimated \$500,000 and two person-years. With a minimal software investment and two weeks' development time, vital statistics were available in a fraction of the time that it used to take to access information, resulting in faster delivery of benefits to the victims.

Finalist for the Federal CIO Council Excellence.Gov Awards, 2002

U.S. Postal Service (USPS)

To meet the federal requirements of the Bank Secrecy Act (BSA), the USPS needed a system for tracking suspected money laundering activities at more than 39,000 branches selling over \$25 billion worth of money orders annually. Information Builders helped the USPS build an award-winning decision support system for monitoring purchase trends and ensuring compliance with the complex BSA reporting requirements.

This anti-money laundering system was designed as a comprehensive solution to capture suspicious transactions involving money orders, funds transfers, and stored value cards at USPS outlets. The system includes highly sophisticated drill-downs, querying, and reporting to allow postal officials to double-check money orders and ferret out suspicious patterns.

Winner of a GCN Federal Government Agency Award for Excellence, 2001

Finalist for the Computerworld Honors Awards, 2001

State of Pennsylvania

Under Governor Tom Ridge, the state of Pennsylvania developed and implemented a Uniform Crime Reporting (UCR) system that provides instant access to state crime data. The solution provides for the collection and reporting of information from any location with Internet access, including police departments, municipal buildings, schools, libraries, and private homes.

Now everyone, from law enforcement agencies to private citizens, has access to crime information – on demand. In addition to providing standard reports, the system allows citizens to create their own queries for accessing specific crime information by department, by county, or statewide.

Finalist for the eSolutions Awards, 2001

U.S. Department of Agriculture (USDA)

The Processed Commodities Inventory Management System (PCIMS) is an integrated data management system used by three agencies of the USDA: the Agricultural Marketing Service, the Farm Service Agency, and the Food Nutrition Service. It tracks requests for domestic and foreign export commodities against purchases and distributions from inventory.

This application helps employees monitor over \$1 billion in commodities for domestic food programs such as the National School Lunch Program and over half a billion dollars in commodities for export relief programs. The system is critical in managing exports of food products to countries like Bosnia.

Winner of a Government Technology Leadership Award, 2000

U.S. Department of Agriculture (USDA) – Rural Development

The Rural Development office of the USDA has a mission to improve the quality of life throughout rural America. To support this mission, Rural Development runs a financial lending and grants program that provides rural communities with essential public facilities such as water and sewer systems, housing, health clinics, and utilities. Managing a lending volume that rivals the fourth largest bank in the nation, the agency's solution integrates multiple stovepipe systems and supplies consolidated reports on various loan types.

In 1997, congressional inquiries required weeks of data gathering and analysis, only to result in already obsolete answers with an 80 percent accuracy factor. Now similar analysis of its loan portfolio takes only a few minutes to perform, and the accuracy of the data is as high as 98 percent.

Winner of a PostNewsweek Agency Award for Excellence, 2001

Contact Us for More Information

Technology and services to aid your organization in the development of similar applications are available to all federal government agencies through our GSA contract, GS-35F-5034H. For more information, simply call (703) 276-9006 and ask for our Homeland Security Task Force. This team consists of seasoned professionals from both Information Builders and iWay Software. You can also learn more about our solutions by visiting us at www.iwaysoftware.com/government.

Sales and Consulting Offices

North America

United States

- **Atlanta*** GA (770) 395-9913
- **Baltimore**, MD Consulting: (703) 247-5565
- **Boston*** MA (781) 224-7660
- **Charlotte*** NC Consulting: (704) 494-2680
- **Chicago*** IL (630) 971-6700
- **Cincinnati*** OH (513) 891-2338
- **Cleveland*** OH (216) 520-1333
- **Dallas*** TX (972) 490-1300
- **Denver*** CO (303) 770-4440
- **Detroit*** MI (248) 743-3030
- **Federal Systems*** DC (703) 276-9006
- **Hartford**, CT (860) 249-7229
- **Houston*** TX (713) 952-4800
- **Los Angeles*** CA (310) 615-0735
- **Metropolitan*** NY Sales: (212) 736-7928
Consulting: (212) 736-4433, ext. 4443
- **Minneapolis*** MN (651) 602-9100
- **New Jersey*** (973) 593-0022
- **Orlando*** FL (407) 804-8000
- **Philadelphia*** PA (610) 940-0790
- **Pittsburgh**, PA (412) 494-9699
- **St. Louis*** MO (636) 519-1411
- **San Jose*** CA (408) 453-7600
- **Seattle*** WA (206) 624-9055
- **Washington*** DC Sales: (703) 276-9006
Consulting: (703) 247-5565

Canada

Information Builders (Canada) Inc.

- **Calgary** (403) 538-5415
- **Montreal*** (514) 630-1134
- **Ottawa** (613) 233-0865
- **Toronto*** (416) 364-2760
- **Vancouver*** (604) 688-2499
- **Victoria** (250) 995-8674

Mexico

Information Builders Mexico

- **Mexico City** 52-55-91-71-20-54

Europe

- **Belgium** Information Builders (Belgium)
Brussels 32-2-7430240
- **France** Information Builders France S.A.
Paris 33-14-507-6600
- **Germany** Information Builders (Deutschland)
Dusseldorf 49-211-522877-0
Eschborn 49-6196-77576-0
Munich 49-89-35489-0
Stuttgart 49-711-7287288-0
- **Netherlands** Information Builders (Netherlands) Bv
Amsterdam 31-20-4563333
- **Portugal** Information Builders Portugal
Lisbon 351-217-230-720
- **Spain** Information Builders Iberica
Barcelona 34-93-344-32-70
Bilbao 34-94-425-72-24
Madrid 34-91-710-22-75
- **Switzerland** Information Builders Switzerland Ag
Wallisellen 41-1-8394949
- **United Kingdom** Information Builders (UK) Ltd.
London 44-208-9824700

* Training facilities are located at these branches;
additional locations are available.

Australia

Information Builders Pty. Ltd.

- **Melbourne** 61-3-9631-7900
- **Sydney** 61-2-8223-0600

Representatives

- **Austria** FOCUS Informationstechnologie GmbH
Vienna 43-12-1136-3870
- **Brazil** InfoBuild Brazil
São Paulo 55-11-3017-5178
- **China** InfoBuild China, Inc.
Shanghai 86-21-5080-5431
- **Finland** InfoBuild Oy
Helsinki 358-9-7250-2250
- **Greece** Applied Science
Athens 30-210-699-8225
- **Guatemala** IDS de Centroamerica
Guatemala City 502-361-0506
- **Gulf States** • Bahrain • Kuwait • Oman
• Qatar • Saudi Arabia • Yemen
• United Arab Emirates
Al-Gosaibi Information Systems 973-274-090
- **Israel** NESS A.T. Ltd.
Tel Aviv 972-3-548-3638
- **Italy** Selesta G C Applications S.P.A.
Genova 39-010-64201-224
Milan 39-02-2515181
Torino 39-011-5513-211
- **Japan** K.K. Ashisuto
Osaka 81-6-6373-7113
Tokyo 81-3-3437-0651
- **Korea** Unitech Infocom Co. Ltd.
Seoul 82-2-3477-4456
- **Malaysia** Optegra Sdn Bhd
Selangor 60-3-80240188
- **Norway** iSolutions AS
Stavanger 47-81544011
- **Philippines**
Beacon Frontline Solutions, Inc. 63-2-750-1972
Corporate Information Solution 63-2-633-1321
- **Poland** Compfort/Meridian Polska SP
Warsaw 4822-630-2660
- **Singapore**
Automatic Identification Technology Ltd.
65-6286-2922
Legato Solutions and Services Pte Ltd.
65-684-63150
- **South Africa** International Computers S.A. (Pty.) Ltd.
Johannesburg 27-11-2335911
- **Sweden** Cybernetics Business Solutions AB
Solna 46-7539900
- **Taiwan** Galaxy Software Services
Taipei 886-22-3897722
- **Turkey** Istanbul
Erdemsoft 90-212-257-5555
Key Soft Ltd. 90-216-428-5933
- **Venezuela** InfoServices Consulting
Caracas 58-212-763-1653

Toll-Free Numbers

- **Sales and Information** (866) 297-4929
- **VAR and Reseller Information** (800) 969-4636



Corporate Headquarters Two Penn Plaza, New York, NY 10121-2898 (212) 330-1700
www.iwaysoftware.com info@iwaysoftware.com

DN3600593.0404

For International Inquiries +1(212) 330-1700

Copyright © 2004 by iWay Software. All rights reserved. Patent pending. [29] All products and product names mentioned in this publication are trademarks or registered trademarks of their respective companies.



Printed in the U.S.A.
on recycled paper