ACTUATE. The people behind BIRT™

Product Summary: BIRT Page Level and SmartSheet® Security

Product Summary

Security is the most vital function of an information application. Security drives confident decisions, provides visibility and increases accountability. The goal of any information application is to securely get the right information to the right people. In order to achieve this, IT relies on a number of data and content management technologies including those that are built into their transaction applications, relational databases and their enterprise information platform.

The only effective way to manage report scalability, however, is with BIRT Page Level Security (PLS), Actuate's patented technology for accessing personalized report content without burdening the system with excess documents or queries. PLS generates a single-server document that includes security rules for each recipient and offers significant performance, security and maintenance advantages over alternative techniques such as report bursting.

PLS functionality is an option available with the BIRT, BIRT Spreadsheet and e.Report families., which eliminates excessive report generation and reduces IT management problems as user communities grow. BIRT SmartSheet® Security is the name of the PLS equivalent for BIRT Spreadsheet. With its latest release, Actuate has added the option of integrating PLS into its BIRT products, eliminating excessive report generation and reducing IT management problems as user communities grow.

Overview

Content security is the most vital function of an enterprise information application. Security drives confident decisions, provides visibility and increases accountability. The goal of any information application is to securely get the right information to the right people. In order to achieve this, IT relies on a number of data management technologies including those that are built into their transaction applications, relational databases and their enterprise reporting platform. In PLS:

- *One query is executed against original sources*
- *One server-side report document is constructed and indexed according to user permissions*
- *Every user receives a personalized report that includes only the pages they are permitted to see*
- *Every user selects any of their preferred file formats, from web, PDF, Word, or Power Point for publishing to BIRT Interactive Viewer, Excel spreadsheets, SmartSearch or to e.Analysis for further inquiry.*

Actuate has integrated PLS, originally created for e.Reports, into all its BIRT products, making it available to all its BIRT-based applications, dashboards and reports eliminating excessive report generation and reducing IT management problems as user communities grow.

For Actuate BIRT Spreadsheet, there's BIRT SmartSheet Security, the equivalent of PLS for spreadsheets. Again, server load is decreased because one query generates virtually limitless numbers of Excel files, ready for delivery to users with the proper layout and security permissions.

All Actuate products run in the Actuate Rich Information Applications-ready server environment and benefit from its unique progressive design architecture, which empowers every user in the enterprise with access to data presented in an application tailored to their own skill level presented in an interactive, user-friendly interface.

Secure Views of Corporate Information

There are a variety of ways to help deliver the right information to the right people in an organization. Delivering secure content to end users from an information platform is a major concern; an organization's user authentication and authorization roles must first be defined and understood. The technology to secure these users and roles can be implemented within the platform or centralized to serve multiple enterprise applications. Enterprise user authentication methods are not addressed in this document, but it does present a number of approaches to manage secure views of corporate information with Actuate's unique approach to secure content delivery, BIRT Page Level Security, and with its equivalent feature for spreadsheet reporting, BIRT SmartSheet Security.

Many enterprise information applications require a fixed number of views of information that adjust content for the target user. An example of this would be the access rights to an organization's weekly sales forecast. This information is sensitive, as it provides a predictive view of future performance—performance at many levels. Often, individual account managers should only see the accounts for which they are responsible, regional managers should see all the accounts in a given region and vice presidents see all accounts in the organization. Traditionally, this is addressed through one of the following information security mechanisms:

Parameter-driven execution against a database— Here the same report design is used for each of the target users. The design includes an abstracted query that passes parameter values, defining and scoping the information shown in the report's content. The advantage of this approach is that it is relatively easy to create, and in effect, delivers a personalized report for each user. In the above scenario, the weekly Sales Forecast is generated once for each account manager, regional manager and vice president, and each individual forecast statement is stored in a secure environment accessible to only the target recipient.

This approach has the disadvantage of performing many individual queries against the source database and an equal number of content construction and formatting operations. In addition, the management of the resulting output files places a significant overhead load on the system and/or administration staff.

Spreadsheet Plug-ins—Using plug-ins to Microsoft Excel is a similar operation. The plug-in binds Excel to the data source or metadata layer and executes its queries against those sources for each user seeking to refresh their view. Plug-ins provide further management complications as they need to be deployed and installed in each user's local copy of Microsoft Office; at minimum an inconvenience, but for large organizations a potential nightmare.

Bursting—Bursting allows a single request for content to create multiple, individualized output files and to manage and secure each of these files independently. This offers distinct advantages over parameter-driven execution and plug-ins since a single query is typically used to generate the content and the pages are then divided, or burst, into individual output files. However, this still results in the creation and management of many different output files.

Metadata security and on-demand queries—An alternative is to rely on the metadata security to manage access to the underlying database and allow users to execute their requests on demand against this data. In this case, it is the metadata layer that is limiting the content output to include only information that the user is permitted to view. This approach helps reduce the overall number of reports created, as some users will not execute these reports every week, and can also reduce the overhead of centrally managing multiple output files because on demand query results are often transient (not saved) or saved and managed by each end user. Generating fewer reports with less for IT to manage must be weighed against pre-generating the content on a regular schedule. First, the information is often inconsistent due to the constantly changing input to the system. In a forecast scenario, the manager who generates his summary on Friday evening will be given information inconsistent with the report and resulting changes inserted by his employee on Saturday. This requires the manager

to execute the report again before Monday's status call. The second issue is that on demand execution results in an unpredictable server workload, which may introduce unacceptable performance or even interrupted service when the system is stressed, especially at the end of the quarter when the user activity is at its peak. Last, the disadvantage of performing many queries against the source database remains.

BIRT Page Level Security

Actuate offers BIRT Page Level Security, a unique and powerful function that generates a single document, which includes security rules determining which pages a user can see, print or save.

BIRT Page Level Security allows a single piece of content to be generated and deployed that addresses the secure information distribution needs of many users. PLS reduces the load on the underlying data source by invoking a single query. PLS reduces the number of report catalog instances to one. And, because a single document is generated, PLS eliminates the need to secure individual access locations. PLS uses one query and generates one report, yet still restricts the information each individual is allowed to see.

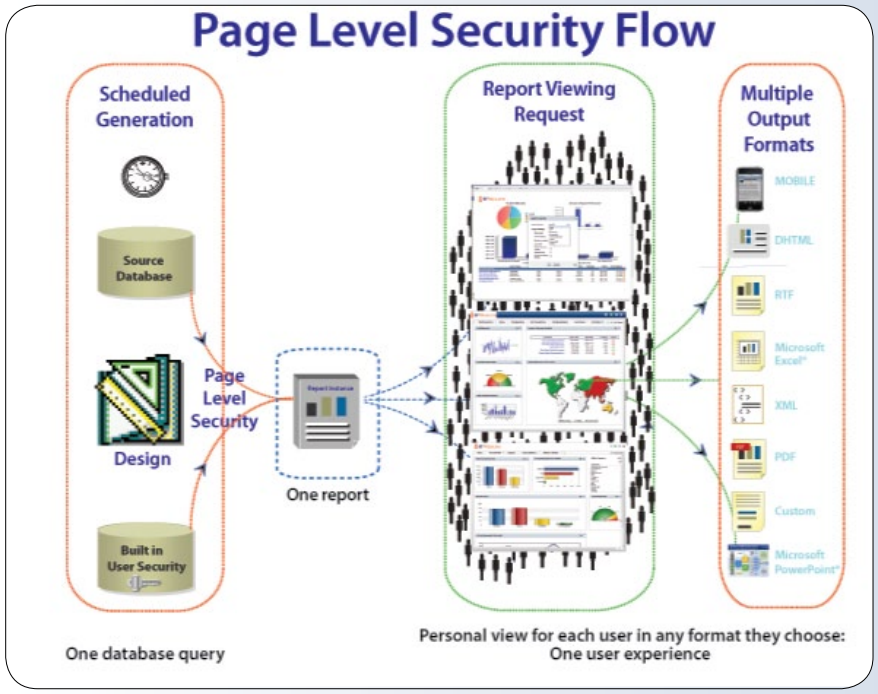
How PLS works

With PLS, the report developer first defines and includes the security rules (users or roles) for the content as the report is designed. These access rights can be driven from external applications, directory services or within Actuate. At generation time, the security rules are used to create an Access Control List (ACL) for each page of the report. The ACL is simply a list of users or user attributes—a user must have at least one of those attributes to view that page.

When the content is viewed, the BIRT iServer retrieves information about the user from the Report Encyclopedia or the external directory. This information is then compared against the ACL for each page of content to determine which pages the user will receive or view.

In our example, the developer of the Sales Forecast has defined a security rule indicating that a given page, the Regional Forecast Summary, is viewable only by the territory's regional sales manager.

At generation time, each Regional Forecast Summary page is assigned an ACL of Northern Manager for the Northern Region page, Eastern Manager for the Eastern Region page, and so on.



Process flow for BIRT Page Level Security: A single report design executes and runs queries against production data sources ahead of time and produces a master report catalog, which is stored on the BIRT iServer. Later, individual users log on to BIRT iServer to retrieve their reports. User privileges are then used to render a personalized report that contains only the data and report components a user is authorized to see.

At view time, the attributes of the user viewing the content are compared to the ACL. When a user attribute matches an element of the ACL, the user allowed to see the page. The attributes for the user are obtained from the iServer (user name and roles) or from an external system such as an LDAP directory. In the example above, if the user has an attribute of Northern Manager, then the user would see the Northern Region page.

Page numbering is automatically handled by BIRT Page Level Security, allowing the developer to easily specify if pages should be numbered relative to the pages the individual can see, or to the whole document.

The BIRT iServer utilizes a high-performance index to determine which pages are available to the user. This provides the same level of performance users experience when viewing content without BIRT Page Level Security—even when it consists of tens of thousands of pages.

Approach	Queries Executed	Reports Viewed	Directories Managed	Report Pages Viewed
Parameter-driven generation and Excel plug-ins	2,600	2,600	50	2,600
Bursting	52	2,600	50	2,600
Metadata on demand*	2,080	2,080	1	2,080
BIRT Page Level Security	52	52	1	2,600

BIRT SmartSheet Security

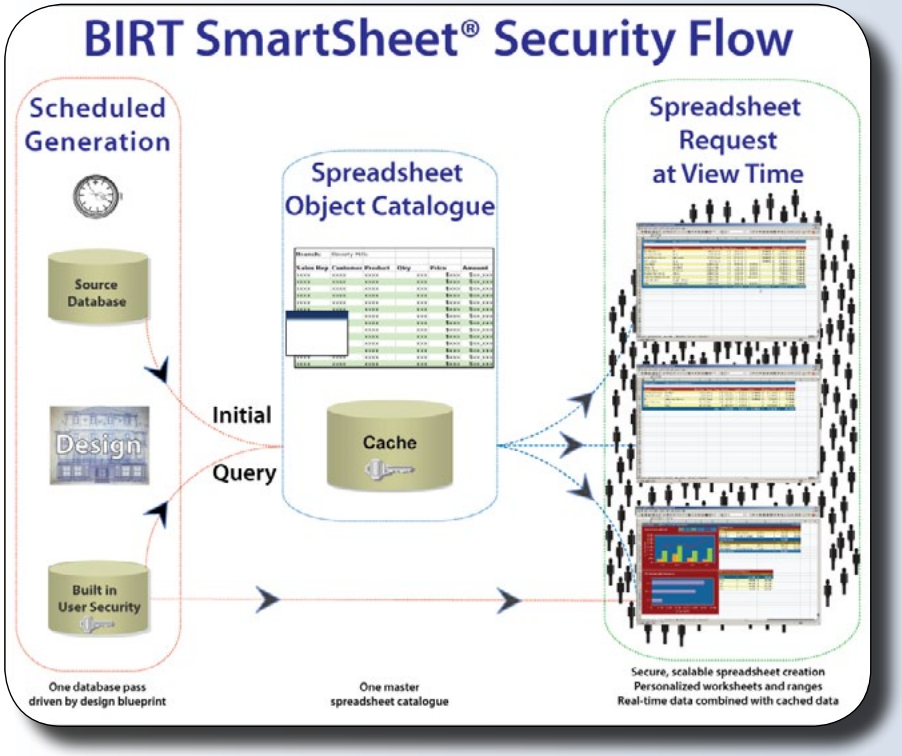
BIRT Spreadsheet offers the equivalent of BIRT Page Level Security with BIRT SmartSheet Security, the only way to automate spreadsheet generation and scale it to vast user communities without overloading the system. BIRT SmartSheet Security's underlying architecture is elegantly simple: A single spreadsheet design drives the queries against source systems in one pass, creating a single master spreadsheet object staged on the iServer. This patented process enables users to access only spreadsheets that contain only the information they are allowed to see, all within a safe, IT-controlled environment ensuring both data control and consistency.

BIRT SmartSheet Security tailors a workbook to each user without re-querying original data sources or re-executing the original design. It dynamically assembles a workbook as the user requests it, which allows it to combine both cached and real-time data, just in time. The result is a fresh, personalized workbook, a fully functional, analysis-ready Excel® file ready for review. This architecture provides a high degree of personalization and scales to thousands of users both inside and outside the firewall.

BIRT SmartSheet Security differs from BIRT Page Level Security in the following ways: First, SmartSheets can manipulate the layout of the workbook as well as the data that fills it. For example, columns, rows, worksheets and data ranges can each be assigned security roles. The second difference is the ability to pass parameters as the user is requesting their Excel spreadsheet; these are called View Time parameters. This powerful feature allows SmartSheets to perform the following as the document is requested:

- *Retrieve real-time data values that can be used within the spreadsheet.*
- *Pass user-supplied filters to the data to further refine what they receive*
- *Pass user or system defined filters*
- *Pass queries to other spreadsheet object catalogues or other external data sources.*

BIRT SmartSheet Security helps resolve one of the oldest problems in computing, how to efficiently deliver Excel spreadsheets to many users without overwhelming IT.



Process flow for BIRT SmartSheet™ Security: A single report "design blueprint" executes and runs queries against production data sources ahead of time and produces a master spreadsheet catalog, which is stored on the BIRT iServer. Later, individual users log on to the BIRT iServer to retrieve their spreadsheets. User privileges are then used to render a personalized Excel® spreadsheet that contains only the data and report components a user is authorized to see.

Deployment Options

BIRT Spreadsheet can be deployed and configured to address the needs of almost any type of reporting project in any business environment:

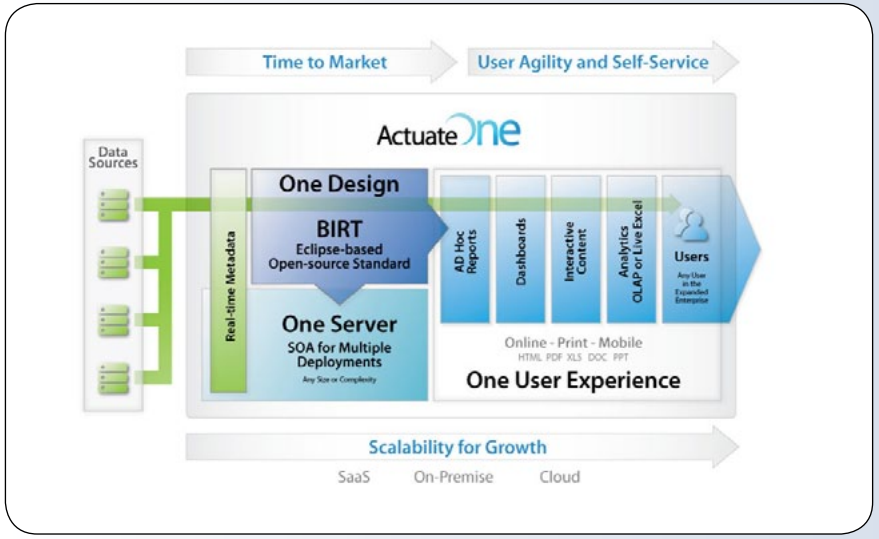
- *Embedded Java Reporting Kit: BIRT, BIRT Interactive Viewer and BIRT Studio can be seamlessly embedded within larger Java applications to provide advanced reporting, printing and formatting features. This option is available to Actuate ISVs and OEMs only.*
- *BIRT iServer Enterprise Deployments: BIRT iServer provides high-scale performance, reliability and security, and supplies BIRT Information Object metadata and multi-server and multi-project capabilities to enterprise collaborative reporting projects.*

The Progressive Design Architecture

BIRT Page Level and BIRT SmartSheet Security BIRT Information Objects are an integral member of Actuate's progressive design architecture, which brings the principles of open source to reporting applications and encourages participation, iterative development and modularity., driving casual user self-service in collaborative reporting.

The entire progressive design architecture includes:

- *BIRT 360: Operational and analytic user-created dashboards for a 360-degree view of the business in a true self-service environment.*
- *BIRT Data Analyzer: In-memory analytics application that helps business users uncover trends, identify anomalies and model scenarios.*
- *BIRT Reports: web reports based on open-source BIRT technology from the Eclipse project, available without charge from BIRT Exchange.*
- *BIRT Studio: self-service, ad-hoc web report development within IT control*



ActuateOne is recognition of a single, common architecture for development and deployment that meets the dynamically changing needs of information consumers.

- *BIRT Interactive Viewer: end user report viewing and customization*
- *BIRT Mobile Viewers: allow users to mobilize and carry corporate information wherever they go.*
- *BIRT iServer: enables the use of BIRT Information Objects, and includes scheduling, versioning, and archiving functions, allowing users to run both on-demand and scheduled reports without IT intervention but within IT-control. This highly scalable implementation of Actuate services provides multi-server, multi-project support; high-availability clustering, failover and load balancing; metadata caching; and enterprise management and tuning features*
- *BIRT onDemand: Actuate's Platform as a Service (PaaS) offering, which enables any user, anywhere, to access enterprise information via the Web, without downloading/installing Actuate BIRT desktop products.*

These options provide an array of choices from which to create unique information applications that appeal to any user.

Within the progressive design architecture structure, BIRT designs can be shared among highly skilled developers, business users and consumers. This encourages participation and supports an iterative development environment, which speeds development and adoption of information applications.

System Requirements

Overall system requirements vary with options chosen. For a system analysis based on your specific needs, please contact an Actuate expert at 1-800-914-2259 (US & Canada) or contact us by *email*. You can also contact one of our *offices worldwide*.

For More Information

To get more information about Actuate security please contact an Actuate expert at 1-800-914-2259 (US & Canada) or contact us by *email*. You can also contact one of our *offices worldwide*.

ACTUATE. The people behind BIRT™

Actuate Corporation
2207 Bridgepointe Pkwy., Ste. 500
San Mateo, CA 94404

Tel: (888) 422-8828
Web:http://www.actuate.com
http://birt-exchange.com