



eTrust® Identity and Access Management Toolkit

The eTrust® Identity and Access Management Toolkit combines an easy to use, flexible SDK with a centralized management server. This enables an inside-out approach to application security by providing comprehensive identity, fine-grained access and security auditing components for developers to embed directly into their applications while externalizing policy management. Use of pre-built, best practices components saves significant development costs while helping the applications meet the highest compliance and security standards.

Key Features at a Glance

- Fine-grained Entitlements for Application-specific Resources
- Embed Distributed Policy Decision Points in Applications
- Centralized Administrative Management Interface
- Secure Audit of Granular User and Administrator Actions
- Standards-based Integration with 3rd Party Provisioning Solutions
- Integration with eTrust® SiteMinder®, eTrust® Admin and eTrust® Security Command Center

Raising the Bar on Developing Secure Applications

Organizations face increasing pressure from regulations such as Sarbanes Oxley, Basel II and HIPAA to improve the security of their entire IT enterprise. The traditional approach to identity and access management (IAM) is to supplement unsecured systems with external, security-specific applications. This approach is a step in the right direction, but it neglects a critical component of the IT infrastructure — internally developed applications.

Fortunately, companies with development organizations have begun to embrace IAM as a fundamental building block to be addressed at the beginning of the development process. However, building

enterprise-strength application security is not a common skill set of most development teams. When attempted, the result is slowed development and inconsistent security capabilities from one application to the next, making administration and maintenance a costly endeavor. Organizations require an approach that will result in rapid development, satisfy the requirement for fine-grained entitlements and allow developers to focus on improving their applications' core competencies.

To address these challenges, CA offers the eTrust Identity and Access Management (IAM) Toolkit. The eTrust IAM Toolkit increases business agility and reduces application costs by providing an SDK for developers to embed fine-grained entitlements while externalizing policy administration functions.

The eTrust IAM Toolkit complements traditional off-the-shelf IAM solutions by providing consistent and manageable IAM capabilities across homegrown applications. Applications embedding eTrust IAM Toolkit components are able to integrate with external IAM solutions through standards-based interfaces in addition to automatic integration with other CA security products.

Distinctive Features and Functionalities

A deployed eTrust IAM Toolkit solution consists of two main components: the application or applications with the embedded eTrust IAM Toolkit client component and the eTrust IAM Toolkit Server. The eTrust IAM Toolkit provides an SDK for application developers to use simple API calls to enable authentication, authorization and audit in their business applications. The IAM Toolkit Server allows security officers or business managers to define fine-grained authorization policies on application-specific resources using a simple, web interface or via available administrative API's.

When deployed, each eTrust IAM Toolkit enabled application interfaces with the eTrust IAM Toolkit Server to exchange the latest security policies and deliver secure events to the audit system. At runtime, applications make fast, in-process authorization checks. This allows business rules, such as "user spending limits" or "medical coverage determinations," to be updated without needing to rewrite the applications performing the policy enforcement.

Access/Entitlements Management

Application security cannot be limited to who can access what application. To be effective, security policies must also enforce what specific actions each user can perform on which resources within the application after they have gained access. The eTrust IAM Toolkit provides a

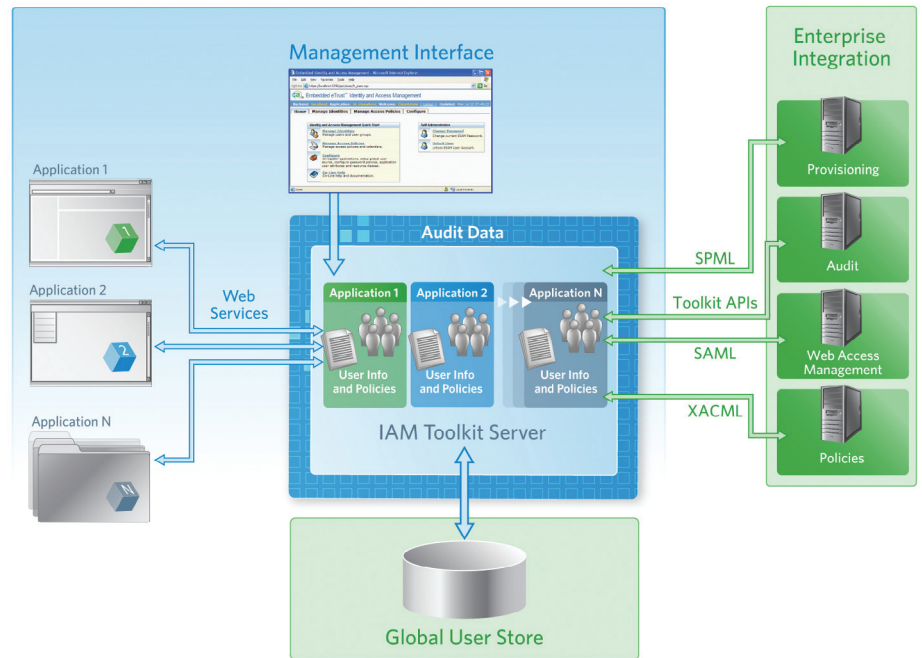


Figure 1. eTrust IAM Toolkit Architecture.

standard means for organizations to implement flexible and granular authorization policies in their business application portfolios.

Fine-Grained Authorizations.

Authorization policies determine what actions may be carried out by which users on what application resources, and under what circumstances. Application developers can define the resources that require security policies as well as the level of granularity needed, then implement the policy decision points with the eTrust IAM Toolkit.

Obligations. Special policies can be used to return required actions to the business application upon an authorization check, allowing the application to use the eTrust IAM Toolkit policy engine to help drive workflow processing based on authorization results.

In-Process Authorization Checks.

Entitlement policies are securely cached in the embedded eTrust IAM Toolkit portion of the application, then evaluated

and executed locally within the application. This enables superior performance and the enforcement of access policies for offline applications.

Calendar Support. Access policies can be defined with time-based criteria such as standard working hours. Delegation policies can also have start and stop times to provide the necessary control to make delegation processes useful.

Separation of Application-Specific Policies. The eTrust IAM Toolkit segregates application-specific policy data in its central repository to ensure separation of policies and administrative controls while enabling application management flexibility.

Events Management

Monitoring, analyzing and reporting on the use of the data contained within corporate applications is a critical component to meeting regulatory compliance. The eTrust IAM Toolkit provides great flexibility to define what

events to capture, promotes a consistent security event format across applications and integrates with audit collection tools for superior analysis and visualization of reports.

Comprehensive Audit. Organizations can choose to capture some or all of their authentication and authorization events. Business rules can be defined at a granular level to selectively capture significant events, for example, "Capture all failed authentications and the first successful authentication after failed events".

Audit Policy Definition and Changes. In addition to auditing end-user actions, the eTrust IAM Toolkit Server can capture every administrative action affecting access security policies.

Interface to Audit Systems. Out-of-the-box integration with eTrust Security Command Center allows all significant authentication and authorization events to be viewed graphically as part of an end-to-end identity audit. eTrust IAM Toolkit applications can also deliver security or other application-related events to event collection systems including eTrust® Audit.

Identity Management

Securing application-level business logic adds an additional dimension to user definition. The eTrust IAM Toolkit provides business application developers with powerful tools to manage application-specific user attributes and group memberships for use in authorization checks. The solution also allows organizations to be confident that their authorization checks are always made on current user profile data.

Global Users. The eTrust IAM Toolkit maintains a consolidated view of all users from a single authoritative source of authentication. Access policies may be based on attributes and group membership of users.

Single Identity Repository. The eTrust IAM Toolkit includes a repository that can be used as the single authoritative source of user identities. As an alternative, this single source can be an external directory such as Microsoft Active Directory, Novell eDirectory or SunONE Directory.

Dynamic Groups. Group membership can be determined through policy evaluations rather than explicit association of each user with the needed groups.

Enterprise Integration

Achieving consistent identity and access management across a complex suite of business applications requires security tools that are adaptable, flexible, manageable and available in the current development environments.

Third Party Integration. Promotes integration with third-party provisioning and management products using industry standards including SAML for identity federation, SPML for provisioning, XACML for access policy sharing and LDAP for directory interface.

eTrust SiteMinder Integration. Native integration allows eTrust IAM Toolkit applications to access user and group information from the user stores eTrust SiteMinder is configured to use, authenticate using eTrust SiteMinder credentials, and support single sign-on with eTrust SiteMinder sites.

SDK in C#, C++ and Java. The eTrust IAM Toolkit supports development environments in C#, C++ and Java. It is fully documented with C#, C++ and Java references for its authentication, authorization, event management and administrative APIs. It includes sample code and XML scripts plus tutorials on how to embed its security functions into applications.

Administration

The eTrust IAM Toolkit minimizes the cost of establishing and maintaining application security policies, user stores and audit rules by providing a single, web-based management interface. By externalizing security policy administration from the application itself, administrators can maintain consistent security levels as business requirements evolve without re-developing application code.

Shared Web UI. The eTrust IAM Toolkit provides an out-of-the-box web UI that is shared among all applications for managing users and groups and for defining and managing access policies. Alternatively, the eTrust IAM Toolkit SDK can be used to embed administrative UI components into custom web pages.

Administrative Scoping. Administrator permissions can be limited to viewing or working on only certain applications, users, resources or policies.

Delegation of Authority. Individuals can grant to others the use of their own access rights.

Permission Checking. Administrators can test security policies and view detailed policy debug information to ensure they have the desired outcome before making them live.

Supported Environments

The eTrust IAM Toolkit supports a variety of platforms.

The eTrust IAM Toolkit client supports the following environments:

- Windows 2000, 2003, XP, .NET
- Linux Intel: Suse SLES 8, 9 and Redhat 8, 9
- SUN Solaris (Sparc)
- IBM AIX 5.1, 5.2
- HP-UX 11.0, 11.11

The eTrust IAM Toolkit Server runs on the following systems:

- Windows 2000, 2003, XP, .NET
- Linux Intel: Suse SLES 8, 9 and Redhat 8, 9
- SUN Solaris (Sparc)
- IBM AIX 5.1, 5.2
- HP-UX 11.0, 11.11

For more information,
call 1-800-875-9659
or visit ca.com

