



Tivoli. software

SecurIT

A Web Access Management solution providing multiple Authentication features, Transaction signing and Validation



Highlights

- Implement unified user authentication and authorization for online business initiatives
- Deliver consistent Web single sign-on (SSO) to your users across Web applications and beyond, including IBM® WebSphere®, Microsoft®, Oracle®, and many other portal and application environments
- Deploy policy-based access control to your enterprise-wide applications, with the confidence that you can scale to tens of millions of users
- Expand single-domain to federated configurations and Web services security management with the modular IBM Tivoli® Federated Identity Manager offering
- Integrate with IBM Tivoli Identity Manager for user provisioning and expanded self-service options
- Save considerable time and money by extending Tivoli Access Manager for e-Business (TAMeB) with other Authentication capabilities
- Easily accommodate user communities with different authentication requirements and/or mechanisms
- Diminish the effort and complexity of changing user authentication mechanisms, without affecting TAMeB or your Applications
- Easily map authentication tokens to a known TAMeB ID (e.g. certificate)
- Reduce the burden on WebSEAL by offloading authentication to TrustBuilder Server
- Share TrustBuilder Server authentication services between TAMeB and other platforms (Network Access, Applications, SSO, etc.)
- Transaction Validation Services can be combined with Authentication Services on the same TrustBuilder system.
- Transaction Validation services can now easily be shared by multiple applications for increased return on investment (ROI).
- Supports different Transaction Proofing mechanisms
- Supports new Transaction Types by generating a highly-configurable challenge over any transaction or data submitted to it

Achieve robust security for online business and legacy applications

Business leaders face some critical questions about the security of their applications and transactions:

- "How can I deploy easy-to-maintain, consistently secured applications with a unified access control policy?"
- "How can I provide a unified user experience—with features such as SSO—when the number of applications, servers and users I'm responsible for is growing exponentially?"
- "Why is the security of my proprietary applications still inadequate, even though I have committed large amounts of money to it?"
- "How can I address security compliance regulations and audits, when my internal controls for the disclosure of sensitive data seem to be scattered all over the place?"
- "If I invest in an authorization solution for my enterprise today, will I need to "rip and replace" it in the future when I address secure interactions with partners?"
- "Does my business have the resources necessary to effectively implement Web services?"
- "What investments do I need to make in order to offer different authentication mechanisms to my clients simultaneously?"
- "How can I keep control on my development costs, when the market requests for new authentication and Transaction Validation and Signing solutions is always growing?"
- "How can I provide a consistent security service across my applications that can ensure transactions are signed and secured?"
- "How can I ensure financial transactions are secure and not tampered with?"

The IBM Tivoli® Access Manager for e-Business and SecurIT TrustBuilder solution delivers an industry leading platform for access control to web-based applications with out-of-the-box accommodation for almost any authentication mechanism. As such, it acts as a Versatile Authentication server. In addition, the solution provides Adaptive Access Control and Transaction Signing & Validation services.

Solution description

IBM Tivoli Access Manager for e-business (TAMeB) lets organizations control both wired and wireless access to applications and data, and provides Single Sign-On (SSO) capabilities for authorized users. TAMeB integrates with Web applications to deliver a secure personalized e-business experience for authorized users. It includes integrated security for CRM, ERP, and SCM solutions, as well as enhancements for securing J2EE- and .NET-conforming applications. TAMeB also manages growth and complexity, helps control escalating management costs, and directly tackles the difficulties of implementing security policies across a wide range of Web and application resources.

TAMeB supports a number of authentication requirements out-of-the-box, like Username/Password, One-time Password (SecurID) and Client-side Certificates, and provides two interfaces to accomplish other authentication needs:

- A C-level External Authentication interface, formerly called CDAS (Cross Domain Authentication Service)
- An HTTP-based External Authentication interface called EAI

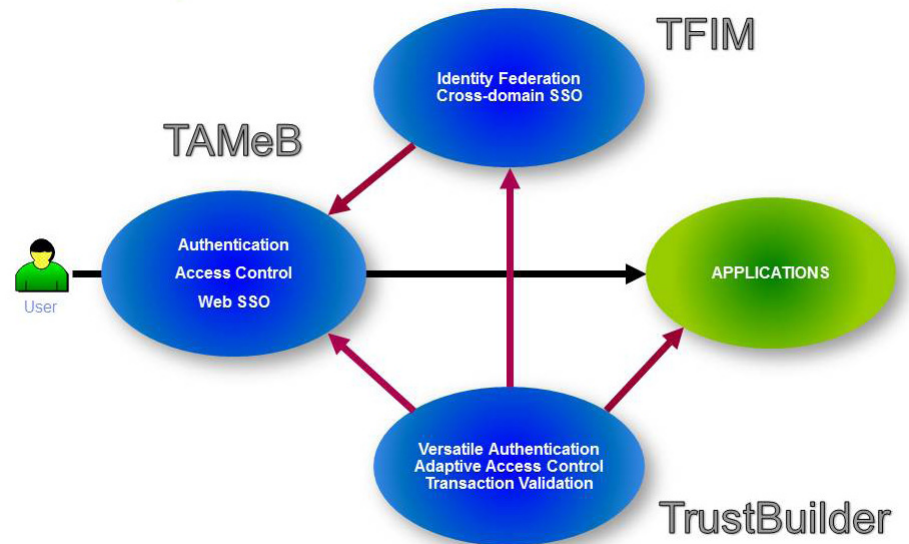
Extending TAMeB's functionality with TrustBuilder adds the flexibility of selecting the appropriate context-based authentication and/or authorization mechanism. Gartner calls this capability "Adaptive Access Control", and it typically includes several or all of the following features:

A Policy-based Workflow capability with

- Context dependant decision making
- Conditional execution based on previous step results

Dynamically evaluate and retrieve

- Authentication validation to be invoked
- Asset criticality/Value
- Time-related conditions
- Endpoint-related conditions
- Network-related conditions



© 2011 IBM Corporation & SecurIT

How it fits together

- Information from other system

React according to Policy

- step-up authentication, increasing the authentication strength
- Invoke additional verification steps in the authentication workflowprocess

Most off-the-shelf Identity and Access Management (IAM) solutions have only partial or limited support for such Adaptive Access Control mechanisms. However, with the IBM Tivoli Access Manager for e-Business and SecurIT TrustBuilder solution, you will have access control to web-based applications with the ability to work with multiple Authentication, context-aware Access Control and Validation mechanisms.

TrustBuilder is a Java-EE-based Security Services framework that provides Authentication, context-aware Access Control and Transaction Validation services to TAMeB and/or applications. The Core platform includes a rules-based policy engine and accommodates both traditional Web and SOA based environments. A plug-in architecture assures simultaneous out-of-the box support for virtually any authentication or validation mechanism, including User Name / Password, One Time Passwords, Digital Certificates, SmartCards, CAP-EMV, Biometrics, etc. Data

from any directory or database can be included in the credential or used for context-aware access control. Digital signing of Transactions can be realized without changing the Application.

Authentication

TrustBuilder Server is an out-of-the-box EAI server, which can easily be configured to fulfill the most complex requirements in terms of authentication. For instance it can itself be involved in the user interaction, in addition to connecting to TAMeB.

The platform can also directly be called by applications or other platforms via regular HTTP/HTML/XML/SOAP interfaces.

TrustBuilder C-Man is able to talk to different TAMeB subsystems like TAM LDAP, TAM Policy server, to the TAM API. Also, it can talk to a back-end authentication server, which makes it possible to integrate TrustBuilder Server with the CDAS interface as well as the EAI-interface.

It is fully compliant with the CJPI to the former CDAS. It runs on the same platforms as WebSEAL, and it supports all the TAMeB authentication mechanisms and features.

TrustBuilder provides TAMEB with a large number of out-of-the-box authentication capabilities:

- UserID/Password using TAMEB LDAP or any other repository
- One-Time Passwords (RSA SecurID, VASCO Digipass, Gemalto Ezio and many more)
- Digital Certificates (SmartCards, Electronic ID Cards, USB, etc.)
- Biometrics (voice, fingerprint, scan,...)
- Proprietary Systems
- Federation Tokens (SAML, ...)
- Software token and mobile token capability

The combination of TAMEB and TrustBuilder provides support for an extensive set of authentication methods and transaction signing and validation, delivering more rapid time to value.

These additions add extensive layered security mechanisms such as the FFIEC guidance for the financial sector (required by many government regulations), combining these authentication mechanisms with Knowledge-based Authentication, Risk/Fraud Analysis or GeoLocation Services.

Transaction Validation

Many customers need to build more proof points into their business applications by safeguarding the integrity of their transaction data and keeping a non-repudiable proof of the transaction's time and date.

Examples of such transactions are:

- payment or wiring transactions in financial applications
- submission of a service request
- proof of delivery for an electronic object or document
- intellectual property

Until now, such proof points had to be built into the application. With TrustBuilder this service is provided, enabling a centralized consistent service to protect

application transactions, and removing the need for custom applications to build this service independently.

TrustBuilder provides the security services needed to create a challenge from the critical data, present it to the user for signing, verify the signature and keep a proof in a non-repudiation store. TrustBuilder supports different signing mechanisms using tokens from VASCO, Gemalto or RSA, compliance with Visa/Mastercard's CAP/EMV standard, and X.509 certificates.

How TrustBuilder enhances TAMEB

- Simultaneous use of multiple Authentication mechanisms
- Workflow-based multi-step Authentication. E.g. first determine authentication mechanism associated to the User, invoke the appropriate validation service and add dynamic data to credential
- Authenticate towards any and multiple backend Repositories. Combine attributes from any backend Repository in User Credential
- Adaptive Access Control at sign-on time
- Transaction Signing and Validation services to applications

Unique Value Proposition

Combining TAMEB with TrustBuilder delivers the following benefits:

- TAMEB with TrustBuilder can be configured out-of-the-box to accommodate virtually any customer requirements for Authentication
- TAMEB with TrustBuilder provides a unique Transaction Signing and Validation capability. These functions don't need to be included in every application, thereby saving application development costs. The transaction's validation and associated integrity can be kept in a non-repudiation store.
- TAMEB with TrustBuilder has proven its product maturity

and enterprise-wide scalability in many large-scale enterprise environments across the world

- Reduce custom application development costs! Provide a consistent service across applications.
- TAMEB with TrustBuilder Server also comes with an easy-to-use Browser-based graphical administration interface to create and manage the workflows and policy.

Many customers present specific authentication requirements. TrustBuilder is the ideal accompanying product for Tivoli Access Manager to fulfill these requirements without laborious, costly custom developments and the associated maintenance burden.

Key Advantages of the combination of TAMEB and TrustBuilder

- Configurable plug-in approach avoids custom coding
- Extended flexibility for adding other Authentication mechanisms
- Off-load the authentication bottleneck from WebSEAL and improve WebSEAL performance
- Allows different Authentication mechanisms to access the same protected resource

This last capability offers a tremendous benefit when an existing user community needs to migrate to another Authentication mechanism. Native TAMEB can only link a particular mechanism to a protected resource, so all users need to change simultaneously. With TrustBuilder this can be handled by policy or under User's control

For more information

To learn more about how Tivoli security management solutions can help you minimize the expense and time of collaborating with business partners, contact your IBM representative or IBM Business Partner, or visit www.ibm.com/tivoli/security or www.ibm.com/partnerworld

About Tivoli software from IBM
Tivoli software provides a set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Helping meet the needs of any size business, Tivoli software enables you to deliver

To learn more about TrustBuilder of SecurIT, contact us or visit our website to learn more about SecurIT solutions please contact us or visit our website www.securit.biz.



© Copyright IBM Corporation and SecurIT 2011

All Rights Reserved

IBM, the IBM logo, ibm.com, Tivoli and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

SecurIT and TrustBuilder are trademarks of SecurIT BVBA in Belgium, other countries or both.

Other product, company or service names maybe trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates. Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.