



IBM Tivoli access management solution for portal and Web security enhanced with SecurIT TrustBuilder delivers out-of-the-box support for almost any authentication mechanism

Enabling secure access in complex Web application environments

Highlights

- Implement unified authentication and authorization for online business initiatives
- Deliver consistent Web single sign-on (SSO) to your users across Web applications and more, including IBM® WebSphere®, Microsoft®, Oracle®, and many other portal and application environments
- Expand single-domain to federated configurations and Web services security management with the modular IBM Tivoli® Federated Identity Manager offering
- Save Time and Money extending IBM Tivoli Access Manager for e-Business (TAMeB) with other Authentication capabilities
- Minimize efforts and complexity when changing user authentication mechanisms, without affecting TAMeB or your Applications
- Reduce the workload on WebSEAL by offloading authentication to TrustBuilder Server
- Minimal impact on existing and new applications, reducing development time

Many organizations have to deal with diverse authentication requirements, often because access to some resources requires stronger authentication than others. However, in practice we see many reasons for this.

One reason may be because organizations desire to leverage existing investments in a system. For example, in merger situations there may be a need to consolidate applications or infrastructure. However, the goal would be to do so without requiring users to change their work habits or requiring many new investments. This is particularly the case in a business-to-consumer (B2C) environment.

Another authentication issue is tied to migration. Even if an organization decides to introduce another authentication method for all its users, the implementation cannot happen overnight in most cases. So there will be a period where certain users are accessing the protected resource using the old means while some others are accessing the new system. In this situation, there is a need to handle the transition smoothly and under user's control.

Traditional authentication mechanisms used for years are today being augmented by new authentication methods and requirements. For example the US FFIEC Guidance for the Banking industry has introduced new security guidelines which should be met by suppliers. In their latest update of the guidance, their advice to customers is to make use of a Layered Security Approach, which involves the use of different controls at different points in a transaction process. This approach can substantially strengthen the overall security of Internet-based services for better results in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses

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

- “How can I deploy secure, easy-to-maintain consistently secured applications that are maintained simply, 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 they 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 in the future?”
- “Does my business have the resources necessary to effectively implement Web services?”
- “Do I need to invest in other solutions to offer different Authentications mechanisms to my clients simultaneous?”
- “How can I keep control on my development costs, when the market request demands for new Authentication solutions keep coming?”

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.

Achieve robust security for on-line business and legacy applications

The combination of TAMEB and TrustBuilder provides a number of valuable out-of-the-box Authentication capabilities along with the all-important flexibility that customers require.

Here’s how it works. SecurIT TrustBuilder provides security services to TAMEB and other environments.

At the *Identity Interface Layer* TrustBuilder provides security services to TAMEB, but also to Network Access Managers and SSO platforms. To this end TrustBuilder supports a number of protocols to handle the requests:

- TAMEB C-level API (formerly CDAS)
- HTML/HTTP, used in case of TAMEB EAI

- SOAP/HTTP (Web Service)
- RADIUS Server
- OCSP Server

In addition, the data format used for the request- response exchange can be configured to accommodate virtually any Resource Manager tool.

At the *Identity Data Services Layer* TrustBuilder ties into a number of back-end systems. These systems will provide TrustBuilder with information to execute these services. Some examples:

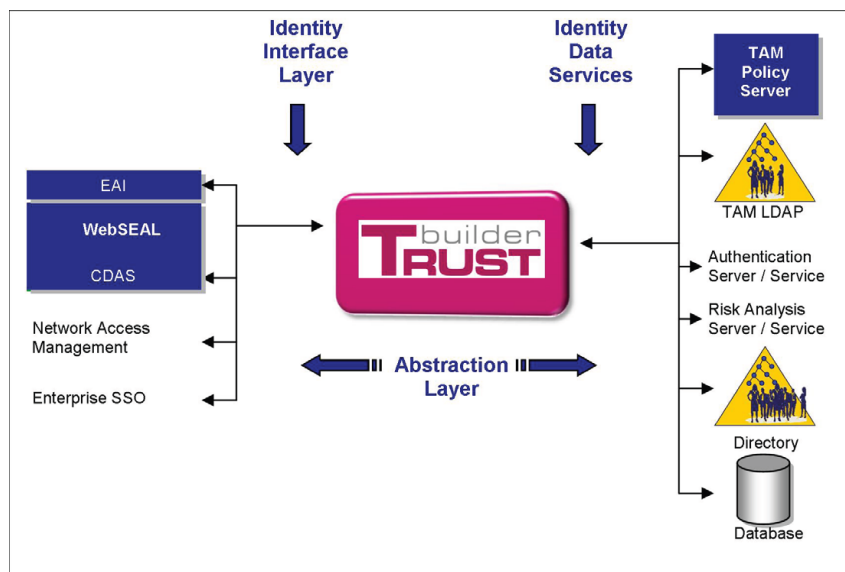
- For authentication, it could use a Radius Server
- For authorization, it could link to a RACF based system
- For Identity Mapping and Validation, it could rely upon an LDAP compliant server
- For gathering additional user profile information, it could access a Database or Web Service.
- The protocols used to communicate with the back-end systems depend on the type of resource that is needed.
- At present TrustBuilder supports a number of protocols with configurable data formats, such as:
- LDAP - RADIUS Client - HTML/HTTP - OCSP Client - SOAP/HTTP - ODBC

These protocols are implemented by plug-ins, called TrustBuilder Back-end Connectors. These are described in an upcoming paragraph called TrustBuilder Connectors.

Using its Rules Engine, TrustBuilder routes the requests it gets from the Identity Interface Layer to the appropriate Identity Data Service. Besides routing, this component can also execute workflows. These workflows can range from very simple to very complex.

Some workflow examples include:

- Validate the data in the TrustBuilder Request (e.g. size)
- Analyze the type of the TrustBuilder Request (e.g. Authentication, Authorization or Identity



A graphical overview of IBM Tivoli Access Manager in combination with SecurIT TrustBuilder

Mapping/ Validation)

- Format the TrustBuilder Response (e.g. format the authentication token)
- Re-route the TrustBuilder Response (e.g. route to other back-end resource)

Example: the following steps provides an outline of a typical TrustBuilder Authentication Request:

1. TrustBuilder receives an authentication request from TAMEB via the CDAS or EAI Interface

2. The Rules Engine picks up the data and analyses it. The authentication data contains a USERNAME and a SECRET

3. Assuming that TrustBuilder is configured to support both Username/Password and Username/One-Time-Password, it routes the USERNAME to ITAM's LDAP server to verify the user's authentication status

4. Upon receiving this information, the Rules Engine re-routes the USERNAME/SECRET to the appropriate back-end service (e.g. TAMEB's native way for Username/Password or a VASCO VacMan Controller for Username/One-Time-Password).

5. Using the validated Identity of the user, additional profile information is retrieved from a back-end Database.

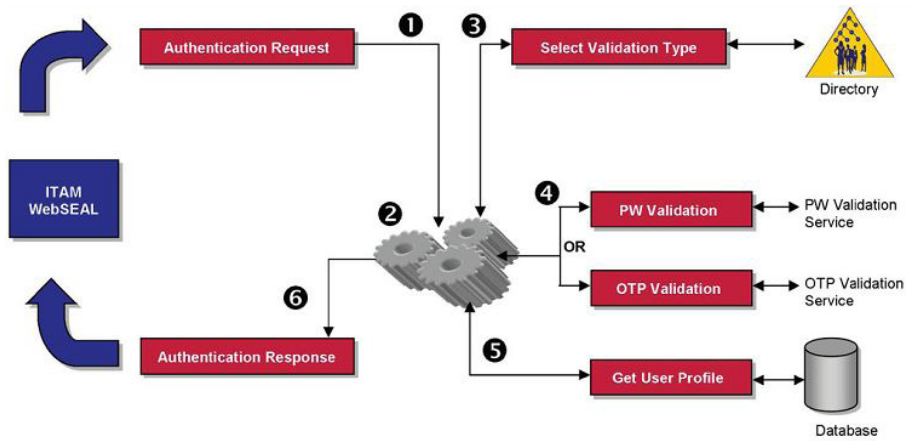
6. The Rules Engine relays the response with the user credential back to the TAMEB.

Extended security services offered to TAMEB by TrustBuilder

A few examples of the extended security services offered to TAMEB by TrustBuilder are:

Authentication Services

Large organizations have authentication requirements for multiple environments, like TAMEB for Web



The outline of a typical TrustBuilder Authentication Request

Access Management, Network Access Management, Enterprise SSO to applications that haven't been web-enabled, and new applications based on the Service Oriented Architecture (SOA) model.

In order to limit the number of "Authentication Islands" one needs to evolve to an Authentication Infrastructure Services model, where data and validation mechanisms can be shared amongst the requesting parties. Amongst others, these services consist of:

- Being able to determine the authentication requirements based on variables, such as the type of User, the Protected Resource, the User's location, content-based variables, etc.
- Simultaneously supporting different authentication mechanisms, like Username/Password with policy, One-Time Password (hardware, software, outbound/mobile), Client Side Certificates (SSL, challenge/response), Biometrics, Knowledge-based Authentication, company-specific variants, etc.
- Allowing the User to migrate smoothly from one authentication mechanism to another. In many cases the mechanism is linked only to the resource a user is trying to access and not to the user itself. This can be a major stumbling block when, for example, an organization is migrating large user communities

from regular password usage to a strong(er) authentication method.

TrustBuilder helps resolve this issue by providing a platform in which multiple authentication mechanisms and sources can co-exist and be combined to suit the most complex authentication needs. Furthermore TrustBuilder provides a unified interface to all these sources, offering the level of abstraction required to mask the peculiarities of different environments. Through its flexible and highly configurable Identity Interface Layer, TrustBuilder can fulfill requests from both today's environments and tomorrow's Service Oriented Architectures.

Access Control Services

Once a User has been properly authenticated, TAMEB will control access to the protected resources. Therefore, it needs Access Control information regarding the User, which is normally stored in its Policy Server.

However, in some cases the information needed to make the authorization decision is not directly accessible by TAMEB. One reason could be that the information is distributed over several sources in the infrastructure and that it needs to be accessed through a variety of protocols.

The system can be configured to provide Adaptive Access Control. This makes it possible to change the enti-

tlement of the user on a per-session basis. TAMEB's Policy server takes care of the static part of the Access Control. But TAMEB also can work with dynamic groups, and TrustBuilder will provide that input at session establishment.

Identity Validation & Mapping services

In order for TAMEB to be able to make an authorization decision, it needs to be aware on whose behalf it should make that decision. Out-of-the-box, TAMEB supports a simple static user credential holding a unique ID and some group or role information. This credential or token is created during authentication and remains valid throughout the duration of the session. This type of credential has the advantage that the back-end applications can easily understand it, but has the disadvantage that it is not secured and, as such, can be tampered with. While credential formats like Kerberos and SAML are good standardization initiatives to arrive at a more common set of tokens, there will always be applications that do not supports these formats. In this case, a mechanism is required to map between token formats.

Furthermore, some applications that deal with very critical data might have a requirement to re-validate a token. For example, the application may want to validate whether the token has expired or whether the token itself is strong enough (e.g. created

based on a strong authentication mechanism) to be used in the context of the resources it is managing.

TrustBuilder provides a platform in which multiple token formats can coexist and converted to each other to better suit these requirements.

TrustBuilder Server can also act as a Secure Token Service (STS) by configuring the Web Service front-end Connector as a WS-Trust Service.

The service will also ensure ID Mapping. This can be based on a rule or a look-up in the TAMEB LDAP or any repository, to determine how and in what way the token has to be mapped to a user known by the TAMEB environment or by the protected application.

These are just a few examples of the service that can be provided by the TrustBuilder platform.

TrustBuilder also provide out-of-the-box software token and mobile token capability. And finally, everything that is required to deal with digital certificates is also provided out-of-the-box along with certificate validation as the revocation checking by any of the methods, locally stored or online access in combination of these methods. And we also implemented a certificate revocation check policy, depending on the user type or the security level that is required or the transaction type. We can determine what level of revocation checking is

acceptable for the transaction. And we can support multiple methods simultaneously. All this is managed by the workflow capability of TrustBuilder by a GUI configuration interface. This capability makes it much easier to configure the system.

TrustBuilder Connectors overview

As stated above, TrustBuilder uses two sets of connectors:

- Front-end Connectors, hosted by the TrustBuilder Identity Interface Layer
- Back-end Connectors, hosted by the TrustBuilder Identity Data Services Layer

All Connectors are pluggable and, as such, only the Connectors that are really required need to be configured. The usage of the Connectors is determined by the TrustBuilder Service Rules Engine under control of the Policy. As such, the system can be configured to accommodate virtually any data, an extremely powerful capability that enables the support of almost any system in no time, both at the Identity Interface Layer and at the Data Services Layer. Connectors themselves are never aware of the way they are used. I.e. they will never have any knowledge of the Authentication, Authorization or Identity service in which they are involved. This means that they can be reused for different services and therefore only need to be configured once.

Front-end Connectors

The choice of Front-end Connectors depends on the context in which the TrustBuilder services will be used.

Back-end Connectors

The choice of Back-end Connectors is influenced by the logic that is required for the Authentication, Access Control or Identity Service. It depends on the appropriate mechanisms that are required and the resources TrustBuilder needs to invoke.

Service Context	Front-end Connector	Communication
CDAS Service	CDAS FE Connector	In this case all TrustBuilder Requests and Responses will be mapped onto proprietary CDAS transactions. (IBM Tivoli Access Manager only)
HTTP Service	Web FE Connector	In this case all TrustBuilder Requests and Responses will be mapped onto HTML/HTTP transactions. Used with EAI.
Web Service	Web Service FE Connector	In this case all TrustBuilder Requests and Responses will be mapped onto SOAP/HTTP transactions.
RADIUS Service	RADIUS FE Connector	In this case all TrustBuilder Requests and Responses will be mapped onto RADIUS Server transactions.
OCSP Service	OCSP FE Connector	In this case all TrustBuilder Requests and Responses will be mapped onto OCSP Server transactions.

The five different options of the Front-End Connectors of TrustBuilder

1. Authentication

LDAP Utility & Authentication Connector

Provides full LDAP client capability to TrustBuilder.

This Connector handles authentication and change password requests for users whose information is stored in LDAP. The LDAP connection can be secured via SSL, supporting both client and server side certificates. The Connector supports most COTS LDAP servers, including but not limited to Lotus Domino, Microsoft Active Directory and IBM RACF.

ITAM Authentication Connector

This connector embeds the ITAM authentication API.

It can be used to authenticate users against the ITAM repository and can also build credentials that can be used by ITAM to authorize users. This connector allows TrustBuilder to be configured as a ITAM EAI Server.

The advantage of using this Connector over the standard username/password authentication is that it allows variations on the standard mechanism, and it can be combined with other authentication mechanisms.

Radius Authentication Connector

This Connector handles authentication requests using the RADIUS protocol.

It communicates with any RADIUS compliant server, such as the RSA Authentication Manager (formerly ACE Server) for SecurID validation.

VASCO DigiPass™ Connector

This Connector handles authentication and change pin requests for systems using the VASCO DigiPass Tokens.

This connector verifies the dynamic password of the used token against the DigiPass data stored in an repository. The returned DN is independent from the username used to log in.

When appropriate (depending on the type of the used token), this Connector allows to change the static pin of a DigiPass token.

The Connector is normally combined with the LDAP Access Connector or ODBC Connector, depending of the chosen repository.

Gemalto SAS Connector

Provides authentication and transaction validation using the OTP solution of Gemalto.

2. Data and Application Access

HTTP(S) / SOAP Connector

This Connector sends requests (such as authentication and change password requests) to a backend server via the HTTP(S) protocol.

The content of the request can be freely formatted as HTML, XML, XML-RPC, SOAP or even name=value pairs, depending on what the backend server expects.

ODBC Connector

This Connector can be used to send any SQL based statements to an ODBC enabled database.

The Connector also supports Stored Procedures.

JDBC Connector

This Connector can be used to send any SQL based statements to an JDBC enabled database.

The Connector also supports Stored Procedures.

Native TCP/IP Connector

This connector creates a TCP/IP channel to a remote service (e.g. a remote connector). The channel can be protected via SSL. The formatting of the data packets can be done using standard functionality of TrustBuilder (e.g. XML and SOAP) or a custom connector can be foreseen.

3. Digital Certificate handling

Certificate Connector

This Connector takes a client certifi-

cate, validates it and extracts attributes if appropriate.

This Connector is usually combined with the LDAP Access Connector to map the owner of the certificate (the Distinguished Name of the subject) to a real user ID. This mapping can be based on rules or a mapping table (stored in LDAP).

Digital Signature Validation Connector

This Connector is used for PKI based challenge-response authentication or transaction signing. It validates a signed token and returns the owner of the signing certificate.

This Connector is usually combined with the LDAP Access Connector to map the owner of the certificate (the Distinguished Name of the subject) to a real user ID. This mapping can be based on rules or a mapping table (stored in LDAP).

OCSP Client Connector

This connector includes an OCSP client that can be used for real-time validation of the revocation status. The connector supports signed requests and responses.

CRL Connector

This connector verifies the revocation status using a local store. The local store is kept up-to-date by means of scheduled CRL and delta-CRL updates.

This schedule is driven by an update policy that can be configured by CA or even by DP (Distribution Point).

Time Stamping Connector

Provides an RFC 3161 (Time-Stamping Protocol) compliant TSP client that be used time-stamp any data available to TrustBuilder. It can also be used to time-stamp auditing data.

STS Connector

This Connector can be used to map between external tokens (e.g. SAML, username/password, certificates, WAM credentials) and generic Trust-

Builder tokens, in both directions. E.g. it allows converting a SAML token into a valid WAM credential. This Connector is usually accessed through TrustBuilder's WS-Trust service.

4. Validation

Challenge Connector

This connector allows TrustBuilder to generate a highly-configurable challenge over any transaction or data submitted to it. For example, this feature can be used for challenge/response based authentication or for signing of critical transaction data.

Crypto Connector

This connector provides a wide range of cryptographic functions like encryption/decryption, signing/signature-validation, hashing, etc.

Non-Repudiation Store Connector

Provides the ability to secure and write any event data into a non-repudiation store. This connector requires an external database.

5. IBM Specific Connectors

The following Connectors have been designed for specific use with IBM Tivoli Access Manager (ITAM). In these cases, TrustBuilder can also run on the WebSEAL reverse proxy (TrustBuilder C-Man version).

Auto-Provisioning/Synchronisation Connector

This Connector can create/modify/delete IBM Tivoli Access Manager user information in the LDAP directory. Possible actions are: changing the password, adding the user to one or more groups, removing the user from one or more groups, changing a user description, etc.

WAS TAI Connector

This WebSphere Trust Association Interceptor provides SSO between ITAM and WebSphere based applications using a secure token.

Lotus Domino Trust Association Connector

The DOMTAI Connector (Domino Trust Association Connector) allows it to use any part of a ITAM credential (including extended attributes) as a basis for SSO between WebSEAL and Lotus Domino. It consists of a local Connector and an authentication plug-in for Notes/Domino, called Domino Trust Association Interceptor.

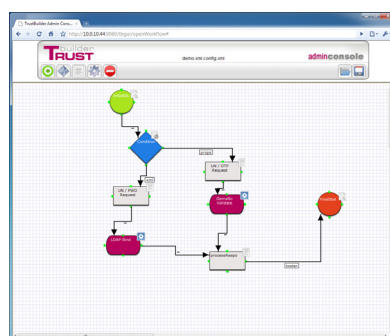
ITAM Administration Connector

This connector allows TrustBuilder to use the administrative functions of ITAM using the ITAM Administration API (e.g. manage users, groups, rights, sessions).

Easy configuration of workflows

The graphical user interface is a browser interface where the admin console can either make a new workflow or import an existing one. And it can all be configured via drag and drop. So the objects can be re-used and, via drag and drop, administrators can determine the way the workflow is being accomplished.

With the TrustBuilder workflow GUI, it is possible to configure the system to select multiple authentication mechanisms, depending on the use case. All these methods can be used parallel. The workflow will determine how and when some of these methods will evoke. It is also possible to link in a particular mechanism to users or user groups, instead of using the mechanism only to protect objects. This is a tremendous added value, for instance,



An example of a simple workflow made with the TrustBuilder GUI

in a migration phase. The GUI tool makes it much easier to migrate users from one particular system to another over a period of time, even on a one-to-one basis and in an automated way if that is required.

How TrustBuilder enhances Tivoli Access Manager for e-Business

- Be able to determine the authentication requirements based on variables, such as the type of User, the Protected Resource, the User's location, content-based variables, etc.
- Simultaneously supporting different authentication mechanisms, like Username/Password with policy, One-Time Password (hardware, software, outbound/mobile), Client Side Certificates (SSL, challenge/response), Biometrics, Knowledge based Authentication, company-specific variants, etc.
- Allowing the User to migrate smoothly from one authentication mechanism to another. In many cases the mechanism is only linked to the resource a user is trying to access and not to the user itself, which can be a major stumbling block when migrating large user communities from regular password to OTP, for example.

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.
- 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.

- TrustBuilder Server also comes with an easy to use Browser-based graphical administration interface to create and manage the workflows and policy.
- The combined solution also offers Transaction Signing and Validation Services.

Many customers present specific authentication requirements. An ideal complement to TAMEB, TrustBuilder can work together with Tivoli Access Manager to fulfill these requirements without laborious, costly custom developments and the associated maintenance burden.

Key Advantages of the combination of TAMEB en 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.

Besides the combination of SecurIT TrustBuilder and IBM Tivoli Access Manager for e-Business, TrustBuilder can also work with Tivoli Federated Identity Manager (TFIM) to add authentication capabilities to TFIM's processes, for instance to log on users who are not included in the Tivoli Access Manager's LDAP.

For more information

To learn more about IBM security solutions for portal and Web environments, please contact your IBM sales representative or IBM Business Partner, or visit www.ibm.com/tivoli/security or www.ibm.com/partner-world

To learn more about SecurIT solutions please contact us or visit our website www.securit.biz. As mentioned above, TrustBuilder can offer Transaction Signing and Validation services to TAM. There is a specific Solution Brief available on our website about this solution.



© Copyright IBM Corporation and SecurIT BVBA 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.