



Transaction Signing & Validation - How it works

IBM Tivoli Access Manager for e-Business and IBM Federated Identity Manager with SecurIT TrustBuilder a secure combination

Highlights

- Implement unified 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
- Expand single-domain to federated configurations and Web services security management with the modular IBM Tivoli Federated Identity Manager offering
- Diminish the efforts and complexity when changing user authentication mechanisms, without affecting TAMeB or your Applications
- 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, allowing significant savings, minimal impact on existing and new applications, reducing development time
- Open to support different Transaction Proofing mechanisms
- Open to support new Transaction Types by generating a highly-configurable challenge over any transaction or data submitted to it

The purpose of Transaction Validation Services

Transaction Signing & Validation is a Layered Security measure that organizations use to accomplish 2 objectives:

- Ensure the critical data in a transaction cannot be altered by malicious hackers, either on the endpoint or in the network
- Maintain an undisputable proof of the Transaction Contents, including a time stamp, in a safe place

Such functionality was traditionally developed inside some business critical applications, such as signing the money wiring instructions in a Web Banking application. Moving this sensitive task into the security infrastructure will facilitate easy re-use of the features, lower development costs and ensure consistency in accordance with business and security policies.

There is an increasing need to re-use such functions into different applications, such as web transactions to request a paid service, registration to events, submitting forms for subscribing to policies, for example insurance policies, or simply keeping an undeniable proof that a user was able to access or obtain particular privileged information at a specific point in time.

This need for secure transactions leads to an architectural choice of offering the re-usable services within the security infrastructure, rather than implementing them individually within each application. In other words: a Service Oriented Architecture.

Bundling this with Authentication Services makes sense because very often the same validation mechanisms will be applied for authentication and signing, but in a different way.

With IBM Tivoli® Access Manager for e-Business and SecurIT TrustBuilder® you will have a leading platform for access control to web-based applications that can accommodate out-of-the-box Transaction Signing & Validation services.

Transaction Validation Phases

Transaction validation is usually handled in three phases: preparation, signing and validation.

In the *Preparation* phase the sensitive data of the transaction is being collected, either from the business application requesting the service or via the data flow from an Access Point (like WebSEAL). TrustBuilder's Challenge Connector allows administrators to define a policy for generating the challenge based on the risk scoring of a transaction, e.g. an amount or the trust level of an account. A challenge is generated based on the security policy configured in TrustBuilder or by parameters included in the request from the application.

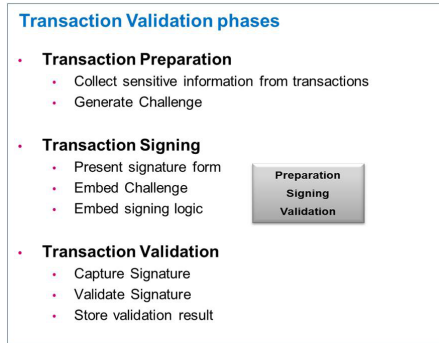
The second phase is the *Signing* of the transaction, which presents a signature form to the user, embedding the challenge that has to be signed and also potentially embedding the signing logic. Different usage models for interaction with the user are possible: either under control of the business application or handled directly by the security infrastructure. The interaction with the user can either be maintained by the applications, using TrustBuilder services as a back-end, or it can be taken over by TrustBuilder until completeness of the signing process.

Finally there is the transaction *Validation* cycle: capturing the signature, validating the signature against the challenge originally produced and, if so required, storing the transaction in a non-repudiated store.

Usage Models

TrustBuilder is able to support different usage models, depending on the desired level of business application involvement. There are two methods supported:

Method (1): The application is involved in all phases of the process.



This method is referred to as the Application-centric use case.

Method (2): The application is not involved in this process. TrustBuilder provides the web service and drives the transaction validation process. This method is referred to as the Application-independent use case.

Whereas the first method is typically meant for new applications, the second method will insert transaction validation in an existing environment without the need to change the application itself. The second method can only be accomplished in combination with an Access Control point such as TAM for e-Business (WebSEAL), where a policy can be set to invoke the transaction validation processes on particular protected objects/transactions.

In the following paragraphs examples are provided about these two use cases, but alternative configurations are also possible, e.g. obtaining the transaction data for challenge generation directly from the business application and subsequently handling the signing and validation phases without further involvement of the application. A different approach for each application or group of applications is possible as well.

	Application-centric approach	Application-independent approach
Typical Use Case	In-house developed or new application	External or COTS application
Features	SOA architecture Transaction Proof <i>can</i> be kept in application domain	Uses TAM Entitlement service Transaction Proof is kept in security domain
PRO	Dynamic challenge generation under application control	No changes to application required
CON	Application changes required	Challenge generation policy by configuration only

Some characteristics of both approaches

Application-centric Use Case

This case shows an application centric use of transaction validation. This actually means that the application keeps control of the user interaction, so it is aware of and involved in each phase of the signing & validation process.

What it means is that we offload all the validation aspects to TrustBuilder Server instead of having to build them into the application(s). TrustBuilder will provide the challenge preparation and the validation service as a back-end service to the application.

During the validation cycle, external functions can be invoked for signature validation, fraud detection or safe storage of transaction data.

Although IBM Tivoli Access Manager for e-Business (TAMeB) is not involved in the Transaction Validation process for this use case, it can still use the Authentication services from TrustBuilder as in many cases the validation mechanism used for authentication and signing will be the same. See also the paragraph 'Signing methods supported'.

Application-independent Use Case

This concept can also be used without involving the application, which is particularly valuable when adding proof points to an existing application, without the need to change it.

In combination with the entitlement functions of TAM WebSEAL, the preparation, signing and validation

cycles can be performed without involvement of the target application. So the application is not aware of the intermediate transaction validation actions.

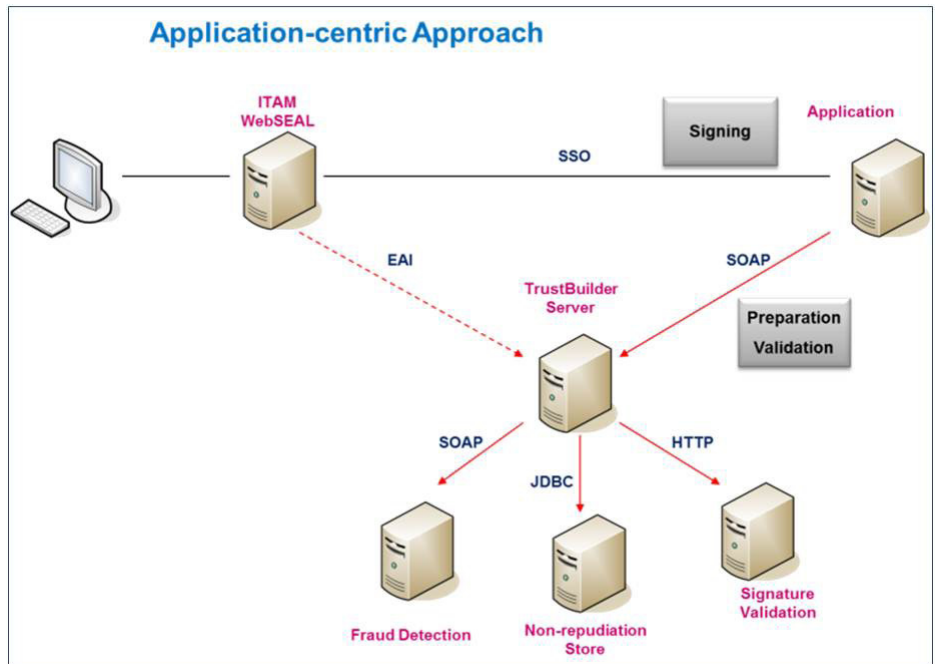
Here is how it works:

Transaction Preparation & Signing

- Tivoli Access Manager Dynamic Authorization Rules
 1. Intercept a critical transaction (URL)
 2. Forwards the transaction details to TrustBuilder (ARS)
- TrustBuilder
 3. Validates the transaction content
 4. Stores the transaction in a Non-Repudiation store (NRS Connector)
 5. Generates the transaction Challenge (Challenge Connector)
 6. Re-directs the user to a transaction signing page

Transaction Validation

- Tivoli Access Manager Dynamic Authorization Rules
 7. Intercepts the signed transaction
 8. Forwards the signature details to TrustBuilder (ARS)
- TrustBuilder
 9. Retrieves the transaction data



10. Validates the transaction signature (Signature Validation Connector)
11. Stores the validation result in the Non-Repudiation store (NRS Connector)
12. Returns the validation result to Tivoli Access Manager

At the end of the process TAMEB concludes that all Access Control conditions are fulfilled and forwards the request to the business application.

Signing methods supported

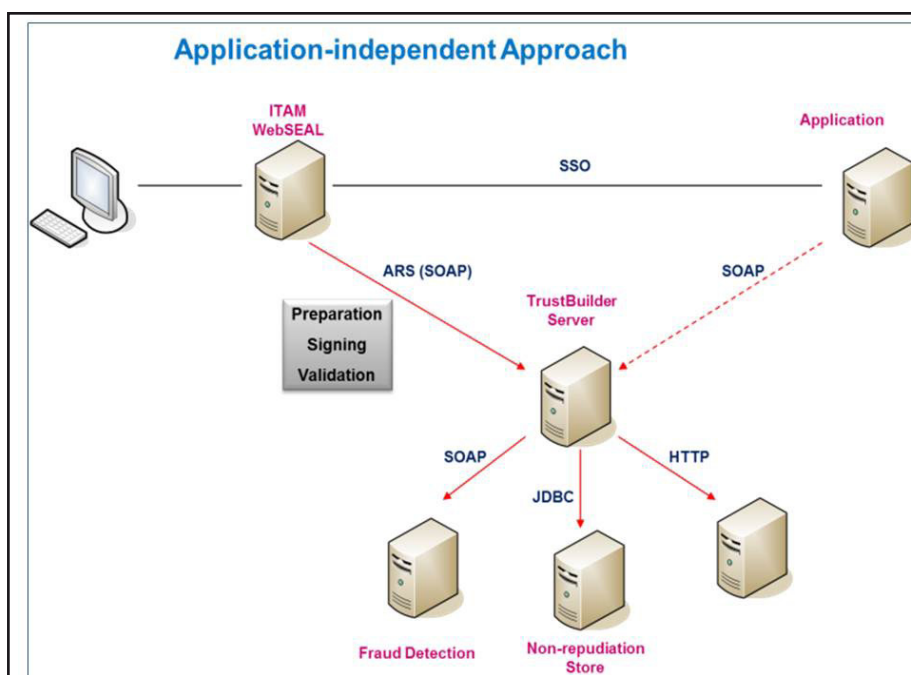
Transaction signing requires the challenge data to be fed into a signing method at the user's location. Depending on the use case, different methods can be selected. Here are some examples:

Using OTP devices with a keypad

- the user enters the challenge into the One Time Password (OTP) device (or alternatively the device obtains it directly from the screen via optical reading)
- the OTP device calculates the one time password based on the challenge and the user's PIN code
- the user commits the transaction by entering this OTP on the signing page

OTP devices can be dedicated hardware from a vendor, for example (but not limited to) VASCO, RSA or Gemalto, or a Smartphone with an OTP application from such vendors. For the financial sector TrustBuilder supports signing in compliance with the CAP/EMV standard from VISA/MasterCard.

The advantage of this method is that the signature is generated on a different device than the user's PC, which is inherently safer and easier to use (no installation or drivers needed).



Using Digital Certificates

This requires some software on the user's PC, albeit downloaded as an applet with the signing page.

- the challenge is picked up by the local software and the user's certificate is retrieved
- the user enters the secret code associated with its certificate to allow its use for signing purposes
- the signed challenge is returned to the central location

The user's signing certificate can be obtained from multiple sources, such as a Smartcard (requires a reader), stored on the user's PC or a USB device.

The advantage of this method is that the user doesn't have to enter the challenge on an external device.

Benefits of the Approach

- Clearly, transaction signing & validation adds another layer of security beyond authentication for business critical transactions. The centralized approach offered by TrustBuilder offloads the process from applications and offers a secure implementation, easily usable by application designers or transparent to the applications.

The solution provides some important and unique benefits:

- Transaction Validation Services can be combined with Authentication Services on the same TrustBuilder system
- Minimal impact on existing and new applications, reducing development time
- Transaction Validation services can now easily be shared by multiple applications, allowing significant savings
- Open to support different Transaction Proofing mechanisms
 - ✓ OTP (Gemalto, RSA, VASCO)
 - ✓ X.509 Signatures
 - ✓ Compliant with CAP/EMV (VISA/MasterCard)
- Open to support new Transaction

Types by generating a highly-configurable challenge over any transaction or data submitted to it .

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. There is a specific Solution Brief Authentication available on our website, www.securit.biz/standard.asp?trustbuilder_for_ibm.



© 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.

Java is a trademark of Sun Microsystems, Inc. in the United States, other countries, or both.

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.