# Attributes: cornerstone to any authorization model

Since the American National Institute for Standards and Technology (NIST) published its 'Guide to Attribute-based Access Control' in 2014, ABAC has only grown in importance. ABAC solves the challenges created by Role-based Access Control (RBAC).

While RBAC may still be used for systems that do not require sophisticated, fine-grained authentication, attributes have become the cornerstone to any authorization model. Even more so as the cloud model has brought more complex authorization rules and new access channels.

Attribute-based Access Control means a user is authorized on the basis of the attributes of an identity rather than on the identity itself or its place in an organization. An attribute can be used in itself, or in combination with other attributes to tighten security.

TrustBuilder Identity Hub combines the openness for organizations to create their own attributes, allowing them to customize security to their own purposes.
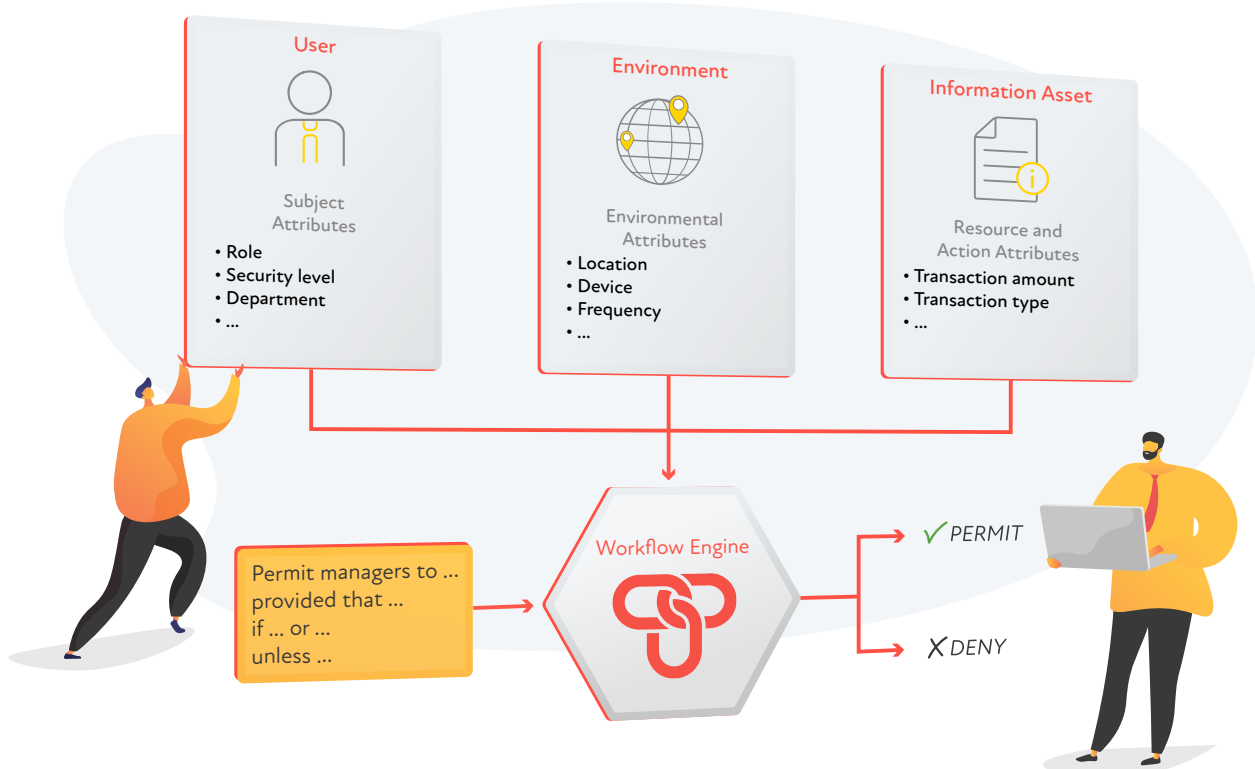
ABAC vs RBAC

- Roles in an RBAC system can become obsolete, when market circumstances change. When companies are acquired or merge, all roles will need to be redefined.
- You can create as many roles as you can, but the number of roles will never suffice to accommodate all use cases. The risk exists of a spaghetti of roles and exceptions to those roles.
- ABAC is the only model that supports contextual information, for instance geolocation, fingerprint, device, access channel, ...
- While RBAC is fine for basic access control, ABAC is the only solution if your security system requires more fine-grained access control with more complex rules.
- A role, as defined in RBAC, can be considered an attribute in an ABAC system.

How TrustBuilder differs

- TrustBuilder combines a powerful rules engine with an unlimited collection of attributes.
- TrustBuilder allows its customers to create their own attributes to authenticate users. Some examples: a retailer setting every product in his inventory as an attribute; an airline using its flight numbers as an attribute, etc. Customers can tailor the solution to their requirements.

Find out more on www.TrustBuilder.com or drop us a line at info@TrustBuilder.com

Workflow Engine in action

- TrustBuilder Identity Hub comes with an out-of-the-box, powerful rules engine, thus eliminating the need for customization.
- Our powerful Workflow Engine contains the rules on what attributes are needed to gain access to a certain application.
- The Workflow Engine supports the set-up of flows between applications, triggered by certain events, which allows data to be transferred smoothly from one application to another.
- The Workflow Engine is the central hub for connections to the different identity stores. Even when the information is distributed over different identity stores, the Workflow Engine will gather and bring together the necessary information for authentication.

By offering Attribute-based Access Control, TrustBuilder Identity Hub allows organizations to play by their own rules.