Knowledge Based Authentication for CA Single Sign-On

What It Does

There are two use cases associated with this packaged work product:

- A user accesses a protected page and has not provisioned their challenge questions and answers
- A user accesses a protected web resource after having entered their questions and answers.

In both use cases the user will first be prompted to enter their normal login ID and password, and if validated successfully get an SMSESSION cookie at the HTML Forms Authentication security level. If they haven't provisioned their questions and answers they will be redirected to a set of web pages that allow them to select a set of questions from a pre-defined list and enter answers to each question.

If, after providing their login ID and password successfully, the module finds that the user has a set of questions and answers available, it randomly selects one or more question and prompts the user to answer the questions. If the user's answer is correct, they are authenticated and get a new SMSESSION cookie at a higher security level.

Knowledge Based Authentication for CA Single Sign-On implements a mechanism called StepUp Authentication, which allows users who have authenticated by plain HTML Forms or Basic Authentication at a lower security level section of a website to only have to answer their Knowledge Based question when they later access resources protected at a higher security level by the Authentication Scheme.

The packaged work product provides its own set of web resources to allow users to provision their questions and answers. If needed, an integration with CA Identity Manager can be provided to enable the component to use the user's Forgotten Password questions and answers for authentication.
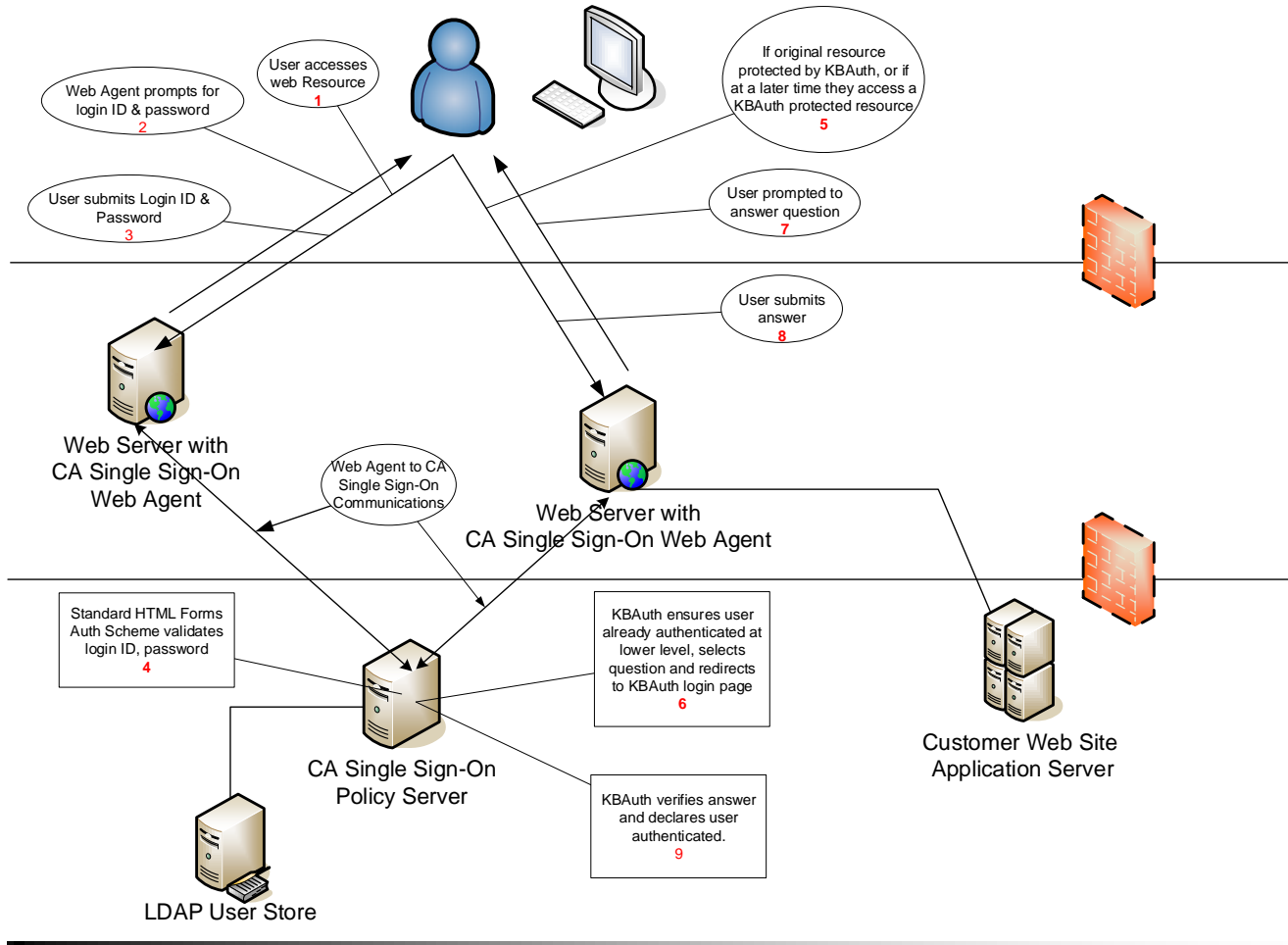
Benefits That Deliver Value

Knowledge Based Authentication for CA Single Sign-On provides:

- An additional level of security beyond username/password based authentication.

How It Works

Typical Authentication Sequence

Web Agent prompts for login ID & password
2

User accesses web Resource
1

If original resource protected by KBAuth, or if at a later time they access a KBAuth protected resource
5

User submits Login ID & Password
3

User prompted to answer question
7

User submits answer
8

Web Server with CA Single Sign-On Web Agent

Web Agent to CA Single Sign-On Communications

Web Server with CA Single Sign-On Web Agent

Standard HTML Forms Auth Scheme validates login ID, password
4

KBAuth ensures user already authenticated at lower level, selects question and redirects to KBAuth login page
6

Customer Web Site Application Server

CA Single Sign-On Policy Server

KBAuth verifies answer and declares user authenticated.
9

LDAP User Store

Technical Prerequisites

A list of technical prerequisites for this packaged work product can be found at **CA Support online**. This is a central repository that will help you identify CA Technologies product compatibility with operating systems, other third-party software products, as well as with certification standards and regulations. **Contact** your CA Services representative for further assistance with purchasing this component.