

AuthEngine: Embedding Strong Authentication in Existing Applications

"It's the most developer-friendly of all products I reviewed. The most unique feature is that they give you the source code to embed into your programs"

-Julius Ang, Managing Director, Digician

Security on Your Own Terms

If you are like many other organizations, you already have applications that maintain sensitive and confidential data that were built by you to meet your own special needs. These may be in-house applications, or applications that you offer to the market as off-the-shelf or customizable software products.

You have your own development and deployment environment that your development team is accustomed to, your own databases, directories, workflow and business logic. What you probably don't have is a means of adding strong, two-factor authentication to the security methods offered in your application

Two-factor authentication provides an extra level of security by eliminating static passwords and replacing them with one-time passwords generated by portable, easy-to-use authentication tokens. This greatly reduces the chances of your system being hacked into, and helps you and your customers meet the authentication requirements being imposed by government and industry regulations and guidelines.

Off-the-shelf authentication servers add too much overhead, and likely are difficult to integrate with your existing environment. Integration is done on their terms, and their system was developed with no knowledge of your workflow, business logic or technical infrastructure.

AuthEngine – Embedded Two-Factor Authentication

CRYPTOCARD's AuthEngine was designed from ground-up to be embedded in existing applications. It is lightweight, easy to implement, and is available in a variety of technologies to fit in with your development and implementation environment.

AuthEngine consists of two components:

1. The **Authentication Module** consists of code that your application will call to authenticate users attempting to login using CRYPTOCARD authentication tokens.
2. The **Initialization Module** is code that you can use to program authentication tokens with encryption keys, seed values, and various other operating parameters such as password length and strength.



AuthEngine

- Fully embeddable authentication solution for custom applications.
- Supports rapid development of authentication capability in web-based applications.
- Enables programming and initialization of industry leading hardware tokens.
- Available as .COM object, .SO shared object or JRE.

AuthEngine appears as simply another authentication method – there are no external dependencies or infrastructure requirements. There are no restrictions on the databases or directories that you integrate with. It can be used along side other authentication methods, and can work with all existing authorization mechanisms.

AuthEngine does not require a dedicated or 3rd-party server, and requires minimal CPU and memory overhead.

Best of all, AuthEngine enables you to integrate strong authentication into your application the way it makes sense to you, allowing you complete control over the workflow, user experience and deployment processes.

Fast Development

It can take less than a week to implement two-factor authentication in an existing application with AuthEngine. A typical deployment will involve:

- 1 – 5 days to implement a basic solution.
 - o Authentication mechanism.
 - o Database changes.
 - o Authentication selection.
- 1 – 2 days to implement self-enrolment, resynchronization and self-help.
- 1 day to implement reporting and audit.

Fits Any Environment

AuthEngine is implemented in the following environments:

- COM Object for Microsoft Windows environments.
- .SO (shared object) for Linux/UNIX environments.
- JRE 1.4 and 1.5 for Java environments.

The AuthEngine SDK also includes a variety of bridges and plug-ins, including a PHP bridge and a freeRADIUS plug-in.

Authentication Token Support

AuthEngine supports the use of the industry-leading KT (keychain) and RB (pinpad) authentication tokens. These tokens are exceptionally rugged and secure, and have replaceable batteries for an unlimited lifespan.

AuthEngine is unique in the market, providing token-based strong authentication fully embedded in existing applications and custom-developed software.

“AuthEngine makes sense as it enables organizations [software vendors, application developers, etc.] to add best-of-breed authentication technology from a recognized market leader. Many organizations simply don’t have the expertise required to develop an authentication solution, and so see it as an area where there is obvious business advantage to partnering with a specialist.”

- Andrew Kellett,
Senior Research Analyst
Butler Group

CRYPTOCARD North America

340 March Road
Suite 600
Ottawa, Ontario
K2K 2E4 Canada

Toll Free: 800-307-7042
Tel: +1-613-599-2441
Fax: +1-613-599-2442
E-mail: info@cryptocard.com
www.cryptocard.com

CRYPTOCARD Europe

Eden Park, Ham Green
Bristol BS20 0EB,
United Kingdom

Tel: +44 870 7077 700
Fax: +44 870 7077 711
E-mail: info@cryptocard.com
www.cryptocard.co.uk

CRYPTOCARD and CRYPTO-Server are registered trademarks or trademarks of CRYPTO CARD Inc. in Canada, the U.S.A. and/or other countries. Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners.
© 2006 CRYPTO CARD Inc.
All rights reserved.

20070103