

# i2 Chooses CRYPTOCard Over Competition

“If any organization is looking for an easy way to escape expensive licensing models, I would not hesitate in recommending CRYPTOCard.”

Stephen DelVecchio, IS Engineer, i2.



## i2 Technologies

Specialists and innovators in Supply Chain Management, with a customer list that includes IBM, 3M, Boeing and more, i2 has made its mark on the industry with solutions that drive out inefficiency and enhance value. Much more than marketing ‘buzz’, i2’s commitment to adding value at every stage often takes staff far afield – from factory floor to head office to wherever their customers do business.

When on the road, i2 workers needed the freedom to securely access data from any location, and developers would frequently be working on client computers (rather than their own laptops). i2 had been utilizing a competitor’s keychain tokens to meet its remote authentication requirements, but felt that the related costs were far too high.

With efficiency and value so important to its corporate culture, i2 management looked for the same from those providing products/services to the company.

## Competitive solution too costly

“Having utilized another provider’s token-based authentication for almost three years, i2 was unhappy that the licensing model would

require repurchasing security tokens every three years,” explained Stephen DelVecchio, IS Engineer, i2.

## CRYPTOCard Solution - Trial

In its effort to find a more cost-effective approach to providing the high-level remote user authentication required, i2 discovered CRYPTOCard’s solution, and decided to take advantage of a free trial download to test CRYPTO-Shield technology.

“It was immediately obvious that CRYPTOCard would provide a 90 percent savings over the competition’s expensive licensing model, and initial testing showed that the technology actually provided increased security and functionality as well,” commented DelVecchio. “For example, i2 would be able to set both the number of potential logon attempts and the complexity of the password, be it numeric or alpha-numeric, to match the security clearance requirements of the specific user.”

i2 began a month-long pilot and was pleased to find that CRYPTOCard’s technology easily integrated with its existing applications and network infrastructure.

## Case in Point...

### The i2 Solution

- i2 was unhappy with need to repurchase/redeploy tokens with their existing supplier
- CRYPTOCard Solutions provided huge savings and increased security
- Installation was carried out in matter of hours
- Migrating users to the new solution is easily handled by the CRYPTO-Shield

## Case Study

### Put to the test

“We put together a matrix to test how well [CRYPTOCARD’s] authentication technology would integrate with i2’s existing security applications, such as Nortel’s SSL VPN and Microsoft certificates, and found no problems,” noted DelVecchio.

But how the solution works for i2 staff is the real test. “i2er’s have to work from clients’ offices, and so, require the ability to connect from client devices,” noted DelVecchio. “The tokens enable i2 to provide special dispensation for employees to access their e-mail and personal files from any available computer,” DelVecchio continued. “This makes it simple for i2 to provide employees with simple access from any computer without any danger of compromising system security.”

During the pilot, i2 selected CRYPTOCARD’s robust metal KT-1 keychain token as a replacement for the plastic keychain tokens it previously had used. The token makes it simple for i2’s staff to positively authenticate themselves by simply pressing a button on the device to receive a randomly-generated password on the LCD display. The user then enters their PIN along with this “one-time” password to positively authenticate themselves to the system. This easy approach made the transition from old provider to new an easy one - no retraining and no adoption period required.

CRYPTOCARD’s event based tokens delivered another advantage: unlike the time-based tokens previously used, which deliver a new password every 60 seconds, users never encounter the frustration of having to logon twice simply because the time-based password expired midway through the process. The event-based model offered another advantage:



i2 is an innovator in the Supply Chain Management arena

“As the password is only displayed when the user presses a button, the token does not remain on at all times, and so the replaceable batteries actually last considerably longer,” noted DelVecchio. In fact, even with frequent use, it’s estimated that token batteries should give a good 5 years of token use.

But the biggest difference of all is that CRYPTOCARD’s tokens are permanent - there is no requirement to replace (and then redeploy) as there was with i2’s former provider. The savings are both obvious and enormous.

## Case Study

### The Roll Out: Keeping it simple

With the month-long pilot successfully completed, i2 began what turned out to be a very simple implementation.

“I completed the installation in less than a day, and when I had a minor issue CRYPTOCARD’s help desk provided great assistance,” noted DelVecchio.

With CRYPTOCARD’s RADIUS server successfully installed within i2’s Nortel VPN, system integration was phased in over the following week. CRYPTOCARD’s simple migration functionality then made it easy to deploy tokens to users in stages over the next month.

“Decommissioned users could simply be imported from the previous provider’s server to the CRYPTOCARD server,” explained DelVecchio. “Then, when the old token is due to expire, it gets replaced with a CRYPTOCARD token, and the user continues with uninterrupted access to the system” DelVecchio continued. “The process is smooth and simple, and there is no related down time at all.”

### From Trial to Roll-out to...

i2 now has 200 remote employees utilizing the CRYPTOCARD tokens and has found it simple to manage the new security solution.

While increasing overall security, i2 has enjoyed significant savings over their previous solution. Overall, trial went well, roll-out went without a hitch and CRYPTO-Shield is managing their authentication needs seamlessly.

### About CRYPTOCARD

CRYPTOCARD is a leader and innovator in the Network Authentication Industry. Its multi-awarded, much-lauded Two-Factor Authentication options include both a server based or ‘product’ solution (CRYPTO-Shield) and a Managed Authentication Service (CRYPTO-MAS). The combination allows organizations of any size and means to adopt a strong authentication policy. CRYPTOCARD is unique in the industry in their commitment to ensuring their products/services work with any common network architecture including OS compatibility (Windows, Linux, Mac OS X), webserver flexibility (IIS, Apache) and database options (Active Directory, LDAP, Open Directory etc). Add to that the outstanding ‘out of the box’ interoperability with many top industry network solutions including Citrix, Checkpoint, Cisco and many more, and you begin to see how CRYPTOCARD has grown since its origin in 1989 to become a thriving enterprise doing business in more than 70 countries.

### 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](mailto:info@cryptocard.com)  
[www.cryptocard.com](http://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](mailto:info@cryptocard.com)  
[www.cryptocard.co.uk](http://www.cryptocard.co.uk)

CRYPTOCARD and CRYPTO-Server are registered trademarks or trademarks of CRYPTOCARD 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 CRYPTOCARD Inc.  
All rights reserved.

20061023