



## Natus Medical Protects New-Born Network

### Background

Founded in 1989, San Carlos, California-based Natus Medical Inc., a manufacturer and marketer of non-invasive, proprietary medical devices and related supplies designed to rapidly screen for common, well-defined disorders in newborns, is creating a platform of screening technologies that can be easily used by medical and non-medical personnel in hospital nurseries, providing for early detection of medical conditions such as hearing impairment. One such development is Natus' ALGO® Newborn Hearing Screener. An ALGO newborn hearing screen can be completed in less than five minutes and may be performed within hours of birth. More than 4000 ALGO units have been sold to hospitals and clinics in the U.S. and overseas.

Natus Medical also assists clinicians in the management of neonatal jaundice. Nearly two thirds of all newborns develop some degree of jaundice within the first days of life. Neonatal jaundice is the single largest cause for hospital re-admission in newborns. Five to six percent of newborns will develop a more serious condition called hyperbilirubinemia. Natus Medical's CO-Stat® End Tidal Breath Analyzer non-

### Organization

Natus Medical

### Industry

Medical

### Requirement

The need to be absolutely certain that only authorized users would be able to access its highly-confidential system.

### Solution

CRYPTOCARD SPT Authentication

invasively detects the presence of hemolysis in neonates, assisting in rapid identification of those at risk for hyperbilirubinemia or other hemolytic disease. Such early detection aids in differential diagnosis and more appropriate follow-up, allowing for cost-effective care and optimal patient outcomes.

To protect sensitive premature babies from excessive sound levels in the NICU, Natus Medical provides MiniMuffs® Neonatal Noise Attenuators. MiniMuffs noise attenuators are specifically designed to reduce noise levels to the baby by at least 7dB, representing a reduction in sound pressure of more than 50%. Fitting gently around the newborn's ears with a special adhesive designed for neonates, Natus Medical's noise attenuators provide a comfortable, easy solution for decreasing noise for babies in the NICU.

---

"CRYPTOCARD's software was easy to integrate within our existing Linux operating system, and enabled users to utilize Macintosh-based computers," Hintz explained. "Additionally, unlike RSA's application where the user's PIN travels across the network in plain text as part of the passcode, the PIN remained local."

*Ed Hintz, Network Systems Engineer*

---

## Birth of a Network

Natus Medical wanted to develop a wireless network that would allow its local and remote employees and consultants, many of whom were not computer savvy, to easily access its highly-confidential data from any location on a daily basis. But, before developing a wireless network, Natus Medical needed to be absolutely certain that only authorized users would be able to access its highly-confidential system.

“Natus Medical would not even consider developing a much-needed wireless network if it could not guarantee high-level security,” explained Ed Hintz, network systems engineer, Natus Medical. “We had to be certain that the development of a user-friendly wireless network would not compromise the security of the existing system.”

The selected security system also had to be cost effective, easy to use, Macintosh compliant, and easy to install within Natus Medical’s existing Linux operating system.

“Macintosh support was important as a good number of Natus Medical’s high-level executives utilize the Macintosh operating system,” Hintz noted.

## Choosing The Right Guardian

With its security wish list clearly defined, Natus Medical began researching Secure Password Technology (two-factor authentication) as a cost-effective method of positively authenticating individual network users. By simply coupling something in the user’s possession (a smart card, a software token, or hardware token), with something the user knows (a PIN) SPT makes it simple for administrators to positively identify both local and remote users attempting to access the network, without complicating the log-on process for time-strapped medical staff.

Natus Medical initially researched RSA’s SecurID token, but was uncomfortable with the fact that the user’s PIN was transmitted

across the wire where it would be vulnerable to a hacker using “sniffer” technology – basically forcing an organization to base its whole security concept on physical possession of the token. RSA’s pricing was also high, and its licensing model forced Natus Medical to re-purchase all tokens every three years due to the token’s limited lifespan. Additionally, RSA did not run on Linux, and could not support the Macintosh operating system.

It was at this time, early in 2002, that Natus Medical looked at a Secure Password Technology solution from CRYPTOCARD. Firstly, Natus Medical was surprised that the initial cost was a fraction of the RSA solution, but that was not the sole reason for Natus Medical’s choice.

“CRYPTOCARD’s software was easy to integrate within our existing Linux operating system, and enabled users to utilize Macintosh-based computers,” Hintz explained. “Additionally, unlike RSA’s application where the user’s PIN travels across the network in plain text as part of the passcode, the PIN remained local.”

Natus Medical was also pleasantly surprised to find that there was no need to replace existing tokens once purchased, creating additional savings. When the token’s batteries expired, the user simply had to replace them.

The server works together with Natus Medical’s existing security applications to make it very simple for all authorized users – both remote and local – to safely access a RADIUS server from any location. Remote users can connect with the network through firewall, RAS/NAS, or VPN while local users can log on via Windows NT, Windows 2000, Windows 98, Windows 95, UNIX logon, or Web server access. Natus Medical can communicate via any combination of dial up, Internet browser, or VPN.

## Child-like Simplicity

Hintz found the server easy to install within Natus Medical’s Linux environment. “It was

easy to integrate the server with our RADIUS backend,” commented Hintz. “The technical support staff was the ultimate in helpful,” Hintz continued. “Instead of giving me pat answers, or simply asking me to read the instructions again, the support staff listened to my questions and responded promptly with solutions customized to my particular system requirements.”

Once installed, the server proved easy to administer. Ideal for today’s highly-dispersed medical workforce, the new server provides centralized authentication with decentralized administration, enabling Natus Medical’s network administrators to add or delete a new user, no matter where they are, in less than a minute. As a result, administrators can ensure new authorized users can gain immediate network access while preventing users who are no longer authorized from accessing confidential medical databases.

“The system’s GUI combined with the “token initializer” makes it easy to create new users or user groups,” said Hintz. “Adding or moving a user is simply a matter of dragging a token from one group folder to another,” Hintz continued. “Also, as CRYPTOAdmin can be run on multiple platforms, an administrator can work on the operating system of their choice.”

The authentication technology also enables administrators to restrict individual-user access down to the web-page level. As a result, user groups can gain complete access to appropriate web pages, but cannot access pages that are designed for a different department.

Additionally, as the server generates a one-time password for every log in, Natus Medical eliminates the significant security management costs associated with administrators having to reset or change existing ‘static’ passwords, or from regularly having to force users to change passwords to protect the network – countering the user resistance often associated with implementing an additional layer of security within the increasingly-busy healthcare environment.

### Affordable Toys

The versatile server platform supports a variety of easy-to-use and reusable hardware and software tokens.

“We [Natus Medical] utilize both the hardware and software tokens in equal measure,” commented Hintz. “The use of the tokens is straight forward and well documented, and users gain the benefit of high-level access security without having to suffer from the inconvenience usually associated with an additional layer of security.”

Natus Medical’s users utilize the RB-1 calculator-style hardware token, the ST-1 pure Java-based software token, and the PT-1 Palm token. A user simply turns on their RB-1 calculator-style token and enters their PIN to view a one-time password in the token’s display. The one-time password is then entered into the dialog box on the user’s PC or laptop – access is that simple. As the unique qualified response is only valid for the current log-on attempt, it prevents would-be hackers from assuming the identity of a valid user by utilizing a guessed or stolen password. Once entered, the server, which runs the administrative database, validates the user’s credentials and Natus Medical is certain that only authorized users gain access to its network.

The software token resides on the user’s PC, and replaces the traditional Windows log-in screen. The user simply enters their PIN, and the token generates the one-time password. The software token provides administrators with click-of-a-mouse deployment – eliminating the significant cost and time requirements of issuing physical (hardware) tokens to be distributed users. Natus Medical finds the software token ideal for users that work on a single PC. The Palm token turns 3Com’s Palm organizer into a one-time-password generator, and Hintz has found the ability to securely connect with the network via cell phone very useful.

“While on vacation, I was informed of a network problem,” explained Hintz. “The Palm token enabled me to utilize my handheld

to securely access the network from my remote location to rectify the situation.”

The server was updated in October 2002, and now supports a multi-function smart card and a smart card reader that fits within the PC-Card slot in the side of the laptop. Users simply have to slide the card into the reader and enter their PIN to gain network access. Natus Medical finds this kind of cutting-edge development enables it to provide its workforce with the ultimate in user friendly, high-level security.

“Presently, our sales department utilizes the software token as it did not want to have to cart around the traditional smart card reader,” Hintz explained. “But with the development of the smart-card reader that fits within the laptop’s port, this drawback has been addressed, and we can now offer the flexibility and increased security of a multi-function smart card without the inconvenience of carrying around a reader attachment,” Hintz continued. “The new reader has eliminated the user resistance to smart cards, and as a result, the sales force will soon be switching to the smart card.”

The token-authentication system, including the server and software, cost Natus Medical less than \$90 per seat – significantly less expensive than RSA’s token system, and nowhere near as costly as a PKI (public key infrastructure), which can run in excess of \$500,000, depending on the size, to build in-house.

### **Proud Father**

The newly-installed authentication system has made it easy for Natus Medical to provide simple real-time remote access to its highly-confidential database.

“Put simply, the database had to be both secure and easy to use,” concluded Hintz. “And now it is.”

---

### **Address**

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

### **Telephone:**

+1 613 599-2441

### **Fax:**

+1 613 599-2442

### **E-Mail:**

info@cryptocard.com

### **Internet:**

<http://www.cryptocard.com>

---