

The Speed of Light and the Speed of Trust



Recently Senetas were partners in a world-first, producing a unique hybrid quantum cryptography solution with Swiss-based technology partner idQuantique. It got me thinking about the speed of light since the new device uses photons and the laws of quantum physics to guarantee the security of data in transmission over optical fibres.

idQ provided the quantum key distribution device and the light photons, Senetas provided the speed and the trust.

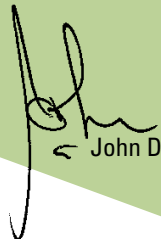
Using our CypherNET high speed network encryptor, a globally-accredited Layer 2 hardware device trusted to secure some of the world's most sensitive data, the hybrid solution gained world headlines, even television news time.

It also demonstrated the nimbleness of both organisations as our joint venture bore fruit in less than six months and the final product is now in customer testing in Europe.

This proof of concept exploits the strengths of both organisations and puts us at the leading edge of new developments in encryption technology. We are excited at the prospects this offers for government and major corporate data security.

Grégoire Ribordy, CEO of idQuantique summed it up saying: "With this joint development, quantum cryptography is now compatible with the requirements of high-speed networks and is ready for large scale deployment."

My headline not only alludes to our success but to the broad philosophies espoused by Stephen Covey in his new book, *The Speed of Trust*, that argues trust is a measurable accelerator to corporate and personal performance. I commend the book to you, as I have to my executive team at Senetas.


John DuBois



SECURED

by **SENETAS**

Issue 1 2007

This issue

Debunking the myth of secure fibre

Best of breed security

Senetas expands reseller channel

10 Gb Ethernet from July 07

Senetas Corporation Limited ABN 33 006 067 607

Head office: Level 1, 11 Queens Road, Melbourne Australia 3004

Phone: 1800 261 114 | +61 3 9868 4555 | Fax: + 61 3 9821 4899

Email: enquiries@senetas.com

Senetas debunks the myth that fibre optic networks are 'inherently secure'

...readily available wiretap device demonstrated

Senetas, the world's leading developer and supplier of high speed network encryption hardware, has exploded the myth that network communications over optic fibre is secure.



Using a readily available coupling device bought over the Internet, Senetas engineers recently were able to tap into a single strand of fibre and extract information.

Senetas has produced a video demonstrating the ease with which information carried over the popular fibre optic data networks can be tapped.

Demonstrating the interception of broadband information – in this case a video with audio streamed over fibre in a simulated corporate network – a coupler clipped on to the fibre was able to simply extract the same quality audio and video signal and send it to a “hacker” laptop.

When Senetas CypherNET encryptors were used to protect each end of the optic fibre, the encrypted video data stream could not be read even with the coupler attached inline.

Senetas CEO John DuBois said the demonstration, using a popular network topology, fibre over Ethernet – known as metro Ethernet – should send a strong message to corporations who were often sold on the myth that optical fibre is inherently secure.

“Clearly we were able to debunk this myth employing a readily available device that takes advantage of a bend in the fibre to extract the signal without damaging the fibre or disrupting communications,” Mr DuBois said.

Using this device someone with mischief or malicious intent can read what's being sent between offices, yet remain virtually undetectable to either the original sender or intended recipient.

Many businesses were sold on the belief that optical fibre is inherently secure because it employed light beams to carry data rather than the usual electrical signals. With more than 480 million kilometres of fibre deployed around the world over the past 25 years and enterprises pumping data along these fibres at up to ten gigabits per second, there's a lot at stake.

“Almost anywhere along those millions of kilometres, company-sensitive data and financial transactions could be extracted,” he said.

Mr DuBois said the global use of metro networks using fibre backbones was estimated to triple by 2009, so the need to secure data-in-motion has never been clearer. Most corporations also run both production and backup systems connected by high speed fibre, so all corporate information is potentially at risk.

He said many businesses still regarded expenditure on security as unnecessary, a reluctant purchase, often agreeing to loosen the corporate purse strings only after a security breach.

“Far from being a low-priority expenditure item, proper security is a business enabler. Unauthorised access to sensitive data not only affects the bottom line of organisations, it damages their public reputation,” he said. Even private fibre optic networks are vulnerable to this type of attack.

“The truth is that even so called ‘dark fibre’ used for point to point network communications is not immune from this type of security breach if it travels through telecommunications pits outside offices, or via switchboards that are not physically secured,” he said.

“The best security for private and business sensitive data carried over fibre is high speed Layer 2 hardware encryption such as Senetas CypherNET SONENT encryptors, developed here in Melbourne and sold to some of the world's most security conscious governments, law enforcement agencies, military and enterprises,” Mr DuBois added.



Andrew Younger, CISSP, Senior Consulting Systems Engineer, Senetas Security with a coupling device.

World-leading hybrid quantum encryption marries Senetas' high speed classic network encryptor with idQuantique's quantum key distributor that uses photons of light and the law of physics to provide unsurpassed data security.



Best of Breed Security Preferred to Multipurpose Devices

Senetas has urged businesses to keep it simple when securing information on their networks.

“Complexity reduces security,” said Senetas CEO John DuBois, citing the decision faced by businesses under pressure to use switches and routers re-purposed to also be firewalls, content filters and intrusion detectors, rather than purpose-built, best of breed, accredited security devices.

Dedicated security devices allow separation of duties, which is critical as networks become more complex, process more data and perform at increasingly faster speed. But they also avoid the single point of failure inherent in the use of integrated devices where one component can compromise multiple functions.

“While vendors of some unified threat management (UTM) equipment point to the cost savings of purchasing only one device to do a number of jobs, the risk is that the quality of each element is not as good as a dedicated device ... you could be buying a ‘Jack of all trades and master of none’ device,” Mr DuBois said.

With recent evidence of banking and telecommunications company’s security breaches resulting in millions of dollars lost, there are very strong reasons to ensure information carried on enterprise networks remains secure – from national and global regulations such as Sarbanes-Oxley (SOX), Basel II (Europe), Gramm Leach Bliley (GLBA) and the Payment Card Industry Data Security Standard, to competitive information, the enterprise’s IP or private customer information, he said.

“The question is: what is a director’s personal liability and what is the corporate cost of disclosure, in comparison with any apparent savings in purchasing a multi-purpose device.”

Mr DuBois also warned organisations that they should clearly understand what was being offered by some Virtual Private Networks.

“The word ‘Private’ offers comfort, but often it does not mean ‘confidential’. Secure to an ISP often means traffic separation of data over shared resources so your data may be segregated, but that is not the same as a secure WAN pipe. All distributed communication must be considered part of public infrastructure and must be secured appropriately, which we believe is only achieved through deployment of a dedicated WAN encryptor such as the globally-accredited Senetas CypherNET,” Mr DuBois said.

“For example metro ethernet is a WAN technology for extending a LAN across a city, a country or the world, but unless specified by your service provider, VPNs are not encrypted, meaning practically anyone who has access to physical infrastructure could view or pullout sensitive traffic,” he said.

Mr DuBois said Senetas partnered with a number of service providers who provided point to point network encryption over Ethernet and optic fibre using CypherNET, which also offered significant speed, data throughput and implementation advantages over networks encrypted using IPSec solutions.

“IPSec is known to increase bandwidth requirements by up to 50%, depending on packet size, is complex to manage and to implement redundancy, plus it has no method to detect path changes. The trend is now to move to secure networks at the lower data layer (Layer 2, rather than the application layer, Layer 3), where a range of network topologies are supported by Senetas’ high speed encryption at up to 10 Gb/sec,” Mr DuBois said.

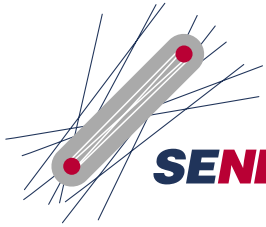
He said the benefits of Senetas CypherNET, which was globally-accredited to the highest government standards and has customers in 27 countries, was its ease of configuration and management.

“Not only is it easy to implement in an existing network, it has lower maintenance costs, the lowest impact on network performance (low latency), is basically set and forget, but importantly it also offers the strongest security and separation of duties,” Mr DuBois said.

He said Senetas had CypherNET encryptors overseas and at a Government Agency in Australia that had been running for three to five years with no downtime.

“With more than 480 million kilometers of fibre deployed around the world over the past 25 years, much of it used in networking, there is significant potential that anywhere along those millions of kilometers, company-sensitive data and financial transactions could be extracted.”

John DuBois, Senetas CEO.



SENETAS Security Summit

Senetas Security Summit Melbourne

“Outstanding Success”

Branding the recent Senetas Security Summit “an outstanding success”, CEO John DuBois said it highlighted awareness of business risks and raised the profile of Senetas as a world-leading technology manufacturer.

Mr DuBois said corporate and government attendees in Melbourne, Canberra, Sydney and Wellington NZ, heard that even Top 10 companies are sometimes unaware of the risks and the potential costs they face.

One of Australia’s Top 10 companies, which had just completed a major security and disaster recovery program, remained blissfully unaware that a telecommunications pit at its front door was a security weak link.

Management consultant, Jed Simms, executive chairman of Capability Management, told the Summit that anyone could have simply lifted the lid on the telecommunications pit and tapped into or cut all telecommunications links to and from the company, “including links to their disaster recovery site.”

Mr Simms said it was a typical example of an organisation that believed it had covered all the potential security risks, yet overlooked the most obvious.

In order, money, compliance, reputation and risk would get senior management’s attention, but concentrating on risk alone rarely worked.

“Managing risk is just one of those things you do in managing a business – it is the least likely of the four to get approval unless you first tackle the other three,” Mr Simms said.

Risk, Return and No Regret

The Director of Risk Programs at Monash University, Michael Vincent said enterprises should factor in the economic cost of “regret” in calculating the real cost of security breaches.

“Most businesses believe that for a given level of risk there must be a given level of return, which is only focused on the upside.

But if the worst case happens, how much will you regret it,” he said.

Mr Vincent said risk management courses at universities such as Monash now taught that businesses should not just rely on the risk/return model but employ the economic model of regret.

“It is like under-insuring: you are very happy when nothing happens that you have had cheaper premiums, but the impact is far greater on business when it does happen if it has not been accounted for. You are applying a very limited parameter in the belief that it is not wrong until something goes wrong, but as a manager you have failed to identify the real value at risk – the cost of regret,” he said.

Business Lessons of War

Colonel Paul Straughair, the Director of Network Centric Warfare with the Australian Army, told the Summit that business could learn the lessons of war.

“The nature of the environment in which the military operates had changed to a technology-based urban landscape.

“Individuals are becoming more lethal: they have the access, funds, innovation and the will to use IT&C Technology, often adapting it for unexpected uses,” he said, citing the use of mobile phones as explosive triggers.

“The military sees its future in the network and devotes considerable resources to network security; the largest military force in the western world can’t stop intrusions entirely, but if you are in business you should employ the same approach to mitigate risk,” Col Straughair said.

Mr DuBois said the idea of the inaugural Security Summit was to provide business with a diverse range of thought leadership about security and business risk.



Summit speakers Straughair, Vincent, DuBois and Simms

If you would like to be informed of future Senetas customer events, send your details to: events@senetas.com



Senetas Expands Reseller Channel

Senetas has appointed France's SmartQuantum SA as a reseller of its high speed CypherNet encryption technology, increasing Senetas' global expansion of sales channels to 27 countries.

SmartQuantum, based in Lannion in the heart of European telecom and optical research, will have non-exclusive reseller rights for France and Benelux – Belgium, Netherlands and Luxembourg.

Senetas CEO, John DuBois said the agreement, signed recently in Paris, represented a significant increase in market coverage for Senetas, given that France had a population of more than 60 million and the Benelux States 27 million.

Mr DuBois said SmartQuantum was a highly regarded encryption specialist, with quantum key distribution technology, which protects the physical transport layer and a unique fibre technology that is able to detect data intrusion.

SmartQuantum CEO, Frederic Coste, said, "Confidentiality, integrity and availability are the key business principles driving the need to secure high bandwidth services and we intend to initially target top industrials' research centers and sensitive communications, data centers (SAN), government and financial institutions".

Senetas has also appointed Saudi Arabia-based Integrated Computer Systems (ICS) as a reseller.

Senetas and ICS have had a marketing collaboration agreement since September 2004 following the awarding of a major \$1.25 million contract to supply a Middle East Government agency with CypherNET ATM encryptors. The contract was delivered by ICS.

Under the two-year agreement which was negotiated recently in Riyadh by Senetas CEO, John DuBois and jointly signed by Mr DuBois and ICS Executive General Manager, Fahad AlZeer, the range of globally-accredited CypherNET encryption hardware will be marketed in the Kingdom of Saudi Arabia with ICS targeting government, military and commercial enterprises in the insurance and banking sectors.

Senetas 10 Gigabit high speed Ethernet Encryptor: global trials from July 2007

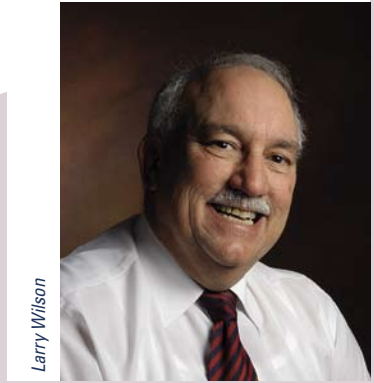
Senetas is expected to deliver its new 10 Gigabit Ethernet (10GbE) encryption platform for testing globally by major customers from July 2007.

CEO John DuBois announced recently that Senetas would further expedite development to satisfy demand for ultra-fast, ultra-secure data transmissions from government and commercial customers.

Mr DuBois said engineers at Senetas' Melbourne head office have been working on the design of the new RoHS-compliant device since November and are on schedule to deliver the new encryptors by July 2007.

Customer acceptance trials for 10GbE begin in the first quarter of Fiscal 2008 and Mr DuBois said there was strong interest in Australia.

The 10GbE device is based on an adaptation of Senetas' existing and proven 10 Gigabit SONET technology, currently in use by a US defence agency.



Larry Wilson

Successful Partnership between IBM and Senetas

The partnership between IBM and Senetas goes back more than 10 years and stretches beyond Australia into South East Asia, India, Hong Kong and the Middle East. Senetas was involved in some of the very early Tivoli implementations and continues to provide specialist design and implementation skills across the Tivoli product suite to IBM and its customers.

Since 1997 Senetas has been the major training partner in the APAC region for Tivoli and established the world's third Tivoli University site in Singapore in 1998 (the others were in North America and the UK).

Senetas has invested heavily in its people and resources to provide superior services and training for IBM and its customers across the Tivoli suite of automation, IT infrastructure management, identity and access management and storage management. All Senetas trainers are fully certified and expert practicing consultants in the implementation of the products in their areas of expertise.

IBM's Regional Manager, ANZ Software Group Services, Darren Reid said: "The power of Tivoli is in quickly adapting to changing environments and evolving business needs. The success and longevity of the Senetas relationship has been because both organisations have been flexible in working together to achieve the best for the customer.

"The value of Senetas to IBM is that they can provide a 'cradle to grave' service for Tivoli implementations covering design, implementation and ongoing support and they can even train the customers in the solution. It makes for a high quality successful outcome for our customers," Mr Reid said

Senetas General Manager – Consulting, Larry Wilson, said Senetas and IBM Tivoli were an ideal fit with Senetas specialising in services that provided and secured enterprise information.

"We assist enterprises to maximise their profitability by providing meaningful information securely and through Tivoli, IBM provides the means to execute on our business promise. We have had a number of very successful joint engagements with customers able to demonstrate significant ROI," Mr Wilson said.

Over the past 12 months IBM has successfully engaged Senetas consulting on major projects at many large customers Australia wide covering many business sectors, including banking, energy, technology and communications, fast moving consumer goods plus government.

"At a State health department, Senetas was engaged by IBM to design, re-architect and implement a complete enterprise wide storage network: a major project that was successfully completed over a number of months.

"For a major multinational insurance group Senetas was engaged by IBM to complete an enterprise wide Tivoli Monitoring solution, while at a utility company, Senetas was engaged to design, architect and implement an enterprise wide security access management solution for the energy company's new web portal solution," Mr Wilson said.

The trusted partnership extends beyond the typical relationship, with Senetas actively participating in IBM beta programs and IBM making beta code software available to Senetas for testing and evaluation.

Senetas has also participated in early release workshops, including the recent release of IBM's TIM/TAM Express and TSM Express products to other IBM business partners to provide the knowledge and essential training in these products.

Mr Reid said, "We are investing a lot more resources into the channel space for sales and marketing.

IBM has actively supported Senetas in joint marketing programs, including direct marketing, event marketing and joint IBM/business partner/customer networking activities."

New Senetas Training



Senetas Training continues to power ahead with new courses offered to Australia's business community, including the new Tivoli Monitoring 6.1 and Tivoli Universal Agent 6.1, regularly scheduled in Sydney and Melbourne.

There is also strong interest in the new Tivoli Access Manager 6.0 courses, again regularly scheduled in both capitals.

Recently Senetas provided customised Tivoli Identity Manager training for a large Bank, but Training Manager, Jim Foster said regular TIM courses open to the general public were also well

attended. And, as always, Tivoli Storage Management courses are in heavy demand.

Mr Foster said Senetas would offer training in the new Tivoli Provisioning Manager product as soon as it is available. For further information email: jim.foster@senetas.com