

Brokat, which has revenues of about 10 million marks (\$6 million), uses its cryptography as a door-opener to sell much more complicated software that securely links conventional bank computer systems to a bank's internet gateways and on-line services. Netscape, Microsoft and computer equipment manufacturers all include encryption in the networking systems they sell to corporations.

But the United States Government blocks American companies from exporting advanced encryption programs, because agencies like the Federal Bureau of Investigation and the National Security Agency fear that they will lose their ability to monitor the communications of suspected terrorists and criminals.

Far from hindering the spread of powerful encryption programs, however, American policy has created a bonanza for alert entrepreneurs outside the United States. Brokat's hottest product is the Xpresso Security Package, a set of computer programs that bump up the relatively weak encryption capability of Internet browsers from Netscape and Microsoft.

Besides America Online, Brokat's customers include more than 30 big banking and financial institutions around Europe. Deutsche Bank A.G. Germany's biggest bank, uses Brokat's software at its on-line subsidiary, Bank 24. Hypo Bank of Munich uses Brokat in its on-line discount stock brokerage operation. The Swiss national telephone company and the Zürcher Kantonalbank are also customers.

Among Brokat's competitors, UK Web Ltd, based in London, is marketing an equally powerful encryption program in conjunction with a Silicon Valley company C2Net Software. Recently, UK Web and C2Net boasted of selling "full-strength" cryptography developed entirely outside the United States.

"We don't believe in using codes so weak that foreign governments, criminals or bored college students can break them," the two companies said in a statement, in a stinging swipe at the American export restrictions.

Bigger companies are starting to jump into the fray as well. Siemens-Nixdorf, the computer arm of Siemens A.G., recently began marketing a high-security Internet server program that competes with products from Netscape. Companies can download the software from Siemens computers in Ireland.

There is nothing illegal or even surprising about this. The basic building blocks for advanced encryption technology, in a series of mathematical algorithms or formulas, are all publicly available over the Internet. American companies like Netscape sell strong encryption programs within the United States, and companies like Brokat are even allowed to export their product to customers in the United States.

For many computer executives, the real mystery is why the United States Government continues to restrict the export of encryption technology. "The genie is out of the bottle," said Peter Harter, global public policy counsel at Netscape, who complained that American policy thwarts his company's ability to compete.

"I have a good product, and I can sell it to Citibank, but I can't sell it to Deutsche Bank," Mr. Harter said. "It doesn't make any sense. Why shouldn't they be able to buy the same product at Citibank? It makes them mad, and it makes us mad."

In response to industry complaints, American officials have repeatedly relaxed the restrictions on encryption over the last several years, and they did so again last November. But because the speed of computers has increased so rapidly, codes that seemed impenetrable just a few years ago can be cracked within a few hours.

In a policy announced last fall, the Clinton Administration announced that it would allow American companies to freely export cryptography that used "keys" up to 40 bits in length. The longer the key, the more difficult a code is to crack. But banking and computer executives say that 40-bit codes are no longer safe and can be cracked in as little as a few hours by skilled computer hackers. The minimum acceptable code, according to many bank executives, must have keys that are 128 bits long.

"From our point of view, there is at least the possibility that a 40-bit encryption program can be broken, and that means there is a danger that our transaction processing could be compromised," said Bernd Erlingheuser, a managing director at the Bank 24 unit of Deutsche Bank. Bank 24 has about 110,000 customers in Germany who gain access to banking services over the Internet using either the Netscape Navigator or Microsoft's Internet Explorer.

Anette Zinsser, a spokeswoman for Hypo Bank, concurred. "Forty bits is just too low," she said. Hypo Bank offers Internet-based banking and discount brokerage services to about 28,000 customers.

In a country not known for high-technology start-ups, Brokat jumped at the opportunity. Mr. Anderer, a former consultant at McKinsey & Company in Germany teamed up three years ago with two fraternity friends, Michael Janssen and Stefan Roever, and two seasoned computer experts, Achim Schlumpberger and Michael Schumacher.

The group originally conceived of building a company around modular software components that were designed for the banking industry, and they financed the company for nearly two years through the money they earned from consulting projects. But they were quickly drawn in the area of encryption, and developed a series of programs around the Java technology of Sun Microsystems.

The Xpresso encryption package is installed primarily on the central "server" computers that on-line services use to send material to individual personal computers. Customers who want to connect to a bank's server download a miniature program, or applet, that meshes with their Internet browser program and allows the customer's computer to set up an encrypted link with the server. The effect is to upgrade the 40-bit encryption program to a 128-bit program, which is extremely difficult for outsiders to crack.

Now, in another step through the looking glass of encryption policy, Brokat is trying to export to the United States. There is no law against that, but American laws would theoretically prohibit a company that used Brokat's technology from sending the applets to their online customers overseas. So the company is now negotiating with the National Security Agency for permission to let American companies send their software overseas, which is where it started from in the first place.

It Brokat convinces the spy masters, the precedent could help American software rivals. "This could open a new opportunity that would benefit American companies if they understand the implications," Mr. Anderer said.

NATIONAL COUNCIL OF SENIOR CITIZENS: KYL AMENDMENT WOULD PUT ELDERLY AND DISABLED CITIZENS AT SERIOUS FINANCIAL AND MEDICAL RISK

HON. FORTNEY PETE STARK

OF CALIFORNIA

IN THE HOUSE OF REPRESENTATIVES

Saturday, November 8, 1997

Mr. STARK. Mr. Speaker, following is a letter from the National Council of Senior Citizens spelling out why the Kyl-Archer amendment is bad for seniors and the disabled and for the Medicare Program.

I urge Members to oppose this amendment. As the public begins to understand what this amendment would do, they will overwhelmingly reject this proposal and the Members who vote for it:

NATIONAL COUNCIL OF SENIOR CITIZENS,
Silver Spring, MD, October 30, 1997.

DEAR SENATOR: The National Council of Senior Citizens strongly opposes any legislation which would reopen the Balanced Budget Act (BBA) for the purpose of limiting or repealing the two-year bar to any Medicare billings after a doctor enters a private payment contract with a Medicare-eligible person. Passage of H.R. 2497, the Medicare Beneficiary Freedom to Contract Act of 1997, would decimate the Medicare program by removing cost protections while reducing the supply of doctors serving the needs of the overwhelming majority of Medicare users.

NCOA opposed, and continues to oppose, the inclusion of the original Kyl Amendment to the Medicare program. Such a provision, allowing a doctor to contract privately for medical care payments outside of the Medicare program, promises to shred three decades of essential quality, consumer, and financial protections which have been incorporated into Medicare.

As enacted, the Kyl Amendment did include the provision barring for two years another Medicare billings subsequent to an agreement for privately-paid Medicare-covered services. Clearly, this could inhibit widespread utilization of the private contract option by many doctors who have not heretofore, in large numbers, declined Medicare payments. Removal of this bar would open the Medicare program to opportunities for many doctors to coerce patients into giving up their Medicare protection in the name of "freedom to contract."

Fewer than 5% of all doctors decline to treat Medicare patients, and only 1% of Medicare beneficiaries have trouble finding doctors. The current doctor-patient Medicare market works well, with no shortage of physicians willing to accept Medicare payments. H.R. 2497 will allow doctors to legally pick and choose patient-by-patient, service-by-service, and dictate payment levels to vulnerable persons needing professional services. Instead of freedom, this would cripple Medicare's ability to hold down health care costs and would put elderly and disabled citizens at serious financial and medical risk.

We pledge every effort to defeat H.R. 2497 or any similar bill and to restore Medicare to its responsibility to cover the costs of an essential set of quality medical services provided by competent doctors and institutions on a uniform and universal basis.

Sincerely,

STEVE PROTULIS,
Executive Director.