



[<< Return to article](#)

A More Anonymous Internet



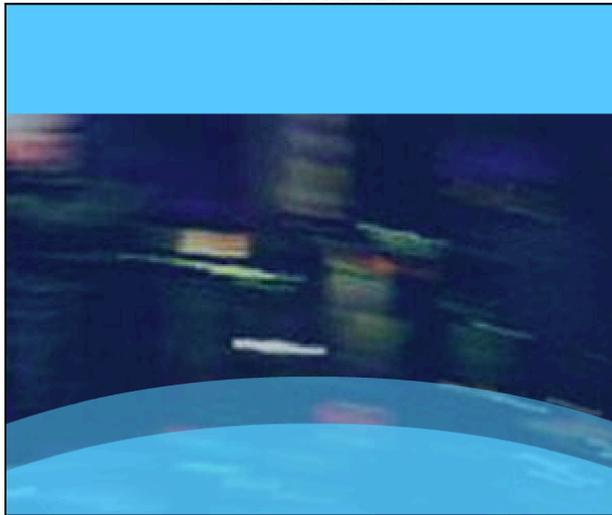
Illustration by James Yang.

By Tracy Staedter
 Innovation
 May 2003

Identity theft and credit card fraud are surging international problems, fueled partly by the need to reveal credit card and Social Security numbers in the course of common Internet transactions. Although most businesses immediately encrypt such numbers, researchers at IBM's Zurich Research

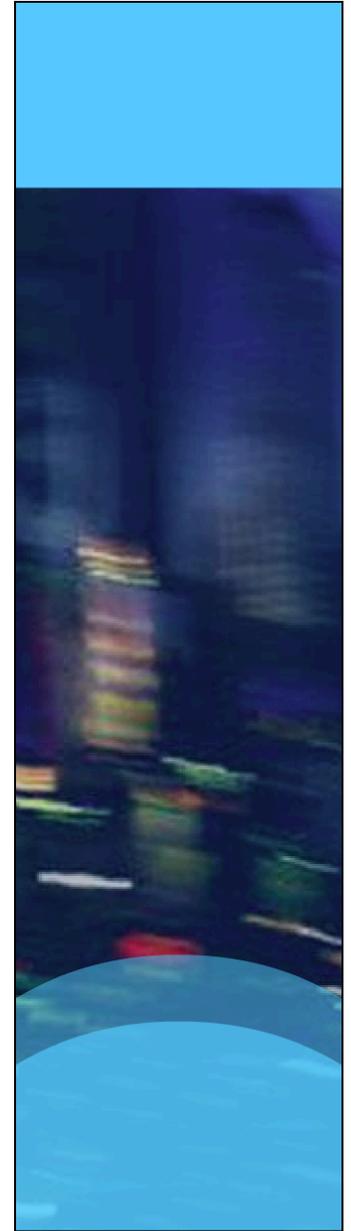
Laboratory and elsewhere are devising ways to avoid having to submit the numbers in the first place.

▼ ADVERTISEMENT ▼



IBM calls its solution Idemix. The software could, for example, allow you to prove to online merchants that you have a valid credit card with certain spending limits, without actually entering the card number. The software starts by enabling you to get an anonymous digital credential from the bank that issued your credit card. This credential contains a pseudonym you choose, the credit card number and its expiration date, and encoded data from the bank that helps verify the credential later.

Then, let's say you want to buy a Kenny G. disc online. The Idemix software in your PC sends information encrypted in the credential to the online music store, informing it that you have a valid credit card. At the store's payment center, another part of the Idemix software reads that information. It uses cryptographic algorithms to confirm bank authorizations and spending limits and to collect payment—all without knowing your actual card number. "This set of techniques is really out in front," says Ronald Rivest, a computer scientist at MIT and a



SPONSORED LINKS

[HP notebooks and desktops.](#)
[Doctor-patient security.](#)

[RHT 2004 Salary Guide – The latest in salary trends!](#)

[Learn about the Qualcomm Launchpad™ Suite of application Technologies.](#)

[Is your salary competitive? RHT 2004 Salary Guide](#)

coinventor of a widely used encryption algorithm. Idemix changes the encrypted version of your credential each time you use it, making it harder for Web sites to track your habits.

Just as banks could issue anonymous credentials, so too could government agencies that issue driver's licenses, Social Security numbers, and other forms of identification. Consider car rentals: an anonymous credential could allow you to prove you are a licensed driver without your having to hand over your actual license. IBM already has prototypes running and could have a version ready for market in one to two years, says Jan Camenisch, lead cryptographer of the Idemix project in Zurich.

Of course, IBM isn't the only company trying to provide secure e-commerce. Credentica of Montreal, Quebec, is also working to commercialize digital credentials for broader applications. And many academic and corporate research groups are pursuing strategies for more anonymity on the Internet. There's good reason for all this research: last year, according to the Federal Trade Commission, 162,000 identities were stolen in the United States alone, and Internet fraud cost consumers more than \$122 million. And someone out there knows you love Kenny G.

Tracy Staedter is the managing editor at *Technology Review*.

Copyright 2004 Technology Review, Inc. All rights reserved