

GARETH BRANWYN JUN 1, 1994 12:00 PM

Digital Signatures

Privacy encryption, the kind found in such software as ViaCrypt/PGP, allows information to be completely hidden from anyone for whom it was not intended. Another popular form of digital cryptography is digital signature software. Rather than hiding your message, it attaches an encrypted "signature" to it, authenticating the electronic document. Adopting a digital signature standard [...]



SAVE THIS STORY

PRIVACY ENCRYPTION, THE kind found in such software as ViaCrypt/PGP, allows information to be completely hidden from anyone for whom it was not intended. Another popular form of digital cryptography is digital signature software. Rather than hiding your message, it attaches an encrypted "signature" to it, authenticating the electronic document.



on the Net will not proceed apace until there's a reliable, and universal means of authenticating documents.

What's the holdup? You'll be sorry you asked.

The question leads straight into a quagmire of bureaucratic red tape and intellectual property disputes. At its heart is a conflict between the government and Public Key Partners, the company that holds the licensing rights to all the critical patents for public key encryption. PKP wants to license these patents to the government in exchange for an exclusive worldwide license of the government's digital signature algorithm patent. That patent was built, to further confuse things, as an "improvement patent" on top of PKP's existing patents for public key encryption.

What we have here is a standoff. The government can't move forward with its encryption technology plans without PKP's patents, and PKP won't license them to the government unless the government hands over the patent and agrees to royalty payments.

Are you following this? After much negotiating, the government and PKP seemed to have finally agreed upon a proposal for a cross-licensing plan - that is, until February 4, when the White House announced that it would be moving ahead with a "royalty-free digital signature standard." What standard is that, and when might we expect it? Nobody knows. Anne Enright Shepherd, a spokesperson for the National Institute of Standards and Technology, would only say that "at this time there is no standard, and negotiations with PKP are ongoing." She did reiterate that administration has determined that such a technology should not be subject to royalty payments.

In the meantime, on March 21, RSA Data Security, a partner company of PKP, jerked the government's chain by announcing that it was making its own digital signature software, called RIPEM/SIG (also based on PKP's patents), available free for noncommercial use and international export. Says Jim Bidzos, president of both PKP and RSA, "You want free signature software, you got it."



licensing it for their commercial products. RIPEM/SIG is available at rsa.com.

ELECTRIC WORD

[Crime-Fighting Computers](#)

[The Watergate Way-Back Machine](#)

[The Dry Lab](#)

[France's Jerry Lewis Media Policy in Action](#)

[Silicon Surfer](#)

[Pay-Per-Play](#)

[Digital Signatures](#)

[A New Sense Organ for the Net](#)

[Tiny Robots Make Light Work](#)

[Plucky Performance](#)

[A Sample Violation](#)

TOPICS ELECTRIC-WORD-ARCHIVE ELECTRIC-WORD-MAGAZINE-2-06 MAGAZINE-2.06

READ MORE



Is It Ever Legal—or Ethical—to Remove DRM?

Digital Rights Management software makes it difficult to copy movies, music, ebooks, and games that you already own. There are ways around it, but breaking DRM opens up legal and ethical concerns.

JUSTIN POT



“We buy homes” companies are procuring disaster-damaged properties for cheap. Survivors say they’re taking advantage of tragedy.

SOPHIE HURWITZ

These Newly Discovered Cells Breathe in Two Ways

In a hot spring at Yellowstone National Park, a microbe does something that life shouldn’t be able to: It breathes oxygen and sulfur at the same time.



How I Learned to Stop Worrying and Love Light Roast Espresso

The traditional knock is that light roast espresso is bitter and sour. But new techniques mean that just plain isn't true anymore.

MATTHEW KORFHAGE



Bluesky has chosen to block access in the state rather than risk potential fines of up to \$10,000 per violation.

MEGAN FAROKHMANESH

Extremist Groups Hated Charlie Kirk. They're Using His Death to Radicalize Others

The Oath Keepers are apparently restarting, and extremist groups like the Proud Boys are calling for “state violence” in the wake of Charlie Kirk’s death.

DAVID GILBERT



US Congressman's Brother Lands No-Bid Contract to Train DHS Snipers

DHS says retired Marine sniper Dan LaLota's firm is uniquely qualified to meet the government's needs. LaLota tells WIRED his brother, GOP congressman Nick LaLota, played no role in the contract.

DELL CAMERON



Authorities have named Tyler Robinson as a suspect in the murder of right-wing influencer Charlie Kirk, citing Discord messages as evidence of his alleged role.

DELL CAMERON

Gear News of the Week: Google's Next-Gen Nest Cams Are Coming, and Sony Debuts a New Xperia Phone

Plus: Qualcomm unveils Quick Charge 5+, Solo Stove has an easier-to-light firepit, Nikon debuts a cinema camera, and xMEMS upgrades the bass on its headphone tech.

JULIAN CHOKKATTU



WIRED Roundup: The US Chip Manufacturers' Bonanza

On this episode of *Uncanny Valley*, our senior business editor joins us to talk about the Trump administration's deals with chipmakers, OpenAI's potential \$500 billion valuation—and ants.

LOUISE MATSAKIS



In the indictment, prosecutors claim Tyler Robinson planned Kirk's killing in advance, citing rooftop surveillance, engraved bullets, and a written note as they seek the death penalty.

DELL CAMERON

 **PRIVACY INFORMATION**