

# Renovating E-Mail With Identity in Mind

BY PAMELA PARKER

That e-mail message may appear to be from PayPal or EarthLink, but is it really? To know for sure, e-mail needs an identity verification system, and there's a growing consensus among e-mail senders and recipients that one should be developed.

The latest two proposals, which were released over the past few days, come from portal giant Yahoo! and e-mail infrastructure company IronPort Systems, which has a partnership with the Network Advertising Initiative's Email Service Provider Coalition (ESPC). Both proposals are chiefly aimed at establishing a technical specification to allow e-mail recipients to verify sender identity. The next step, many in the industry believe, would be to tie a reputation rating — something like a credit report — to that identity. But industry-watchers seem to agree getting beyond e-mail's anonymous nature should be the first step.

"The core issue with e-mail is the lack of identity and the lack of accountability," said Tom Gillis, senior VP of marketing at IronPort.

Yahoo!'s proposed system, DomainKeys, is intended to ensure e-mail communications are really from the domains listed in the sender field. This would allow e-mail administrators to short-circuit messages from spammers and phishers. These scam artists often "spoof", or use the domains and e-mail addresses of, legitimate businesses to lend credibility to their missives and get unsuspecting recipients to open the e-mail.

IronPort Systems has agreed with the ESPC to be one of the "federated registries" to track identity and reputation under the Lumos plan. But it, too, sees a need for a first, baby step.

That's why IronPort this week released a proposal for SMTPi (which stands for Simple Mail Transfer Protocol) with identity features added. Initially, SMTPi would use IP address-based whitelisting combined with extra identification codes in the header to declare the e-mail's campaign, sender, and e-mail service provider.

Senders would have to record those extra identification elements in a central registry and include them in the headers of e-mail messages they send. Receiving systems would look at the IP address of the last server sending the message — the only part of an e-mail header that can't be forged — and check to see if it's present in the registry. If it is on the IP whitelist, the receiver will know to trust the campaign, sender, and e-mail service provider codes.

The second phase in the SMPTi proposal has similar goals to Yahoo!'s DomainKeys, though it goes about the domain authentication in a very different manner. Under SMPTi, domain owners specify, using the DNS, which IP addresses are allowed to send mail claiming to be from a given domain. Then, when recipients get mail they can check to see whether the IP address and the purported domain of the sender match. If they don't, the recipient may want to discard the message.

The third stage, which bears the most

**SMTP**<sup>i</sup>

***IronPort released a proposal for SMTPi (which stands for Simple Mail Transfer Protocol) with identity features added.***

resemblance to Project Lumos, involves the issuance of digital identity certificates and public-key encryption. Senders would digitally sign messages using their private key and embed a certificate in the header of each message. Using the sender's public key, the receiver verifies the certificate and validates the message.

"The problem," says IronPort's white paper on the subject, "is that such a system would require a dramatic overhaul of the existing e-mail infrastructure, requiring years before such a system becomes viable."

Roving Software's Olson predicts Yahoo!'s and IronPort's proposals are just the first among many that will be floated over the next few weeks. While the basic premises will be similar, said Olsen, "there's going to have to be a lot of running around and making sure all the details are the same" before anything can be implemented. "Of course, there will be some balkanization. That's one of the things you just have to get through.

"The network effect is so powerful," she said, "once this begins to be adopted, it's in everyone's best interest to have the same protocols and the same details."



**IRONPORT™**

**IronPort Systems, Inc.**  
1100 Grundy Lane, Suite 100  
San Bruno, California 94066  
tel 650.989.6500 fax 650.989.6543  
email info@ironport.com  
www.ironport.com

#### **ABOUT IRONPORT SYSTEMS**

IronPort Systems is an email infrastructure products and services provider targeting the Global 2000. The company has developed a family of products called Messaging Gateway™ appliances that offer breakthrough performance, unprecedented ease of use, and reduced total cost of ownership. Additionally, IronPort Information Services, Bonded Sender and SenderBase, help guarantee the delivery of legitimate email and thwart the voluminous threat of unsolicited commercial email (UCE) or spam.