OpenEAP: Do it yourself !

The recent initiative launched by Pascal Urien (ENST Paris) combines two main innovations. The first is in the initiative itself. The second is in the EAP cards (TLS, AKA and PSK) that have been developed – the first of their kind – and which are aimed at emerging markets, although they're especially promising for securing Wi-X (WiFi, Wi-Max) and VPN networks, and even beyond, to voice over IP applications. The initial move was unique: "If you don't believe us, try it yourself: download the code from our website, as well as the development and test tools, and do your own card," urges Urien. Somewhat inspired by OpenSSL, OpenEAP is a veritable open architecture, and in fact represents a first in the card sector, which up to now has contented itself with "open-proprietary" systems. The EAP-TLS source code (an authentication method based on the SSL standard), which has already been the topic of a number of discussions among developers, is currently in development, and in its first implementations (for VPN, notably). Efforts are also underway for other methods, such as as AKA (3G, for example, developed by Nokia) and PSK (Pre-Shared Key), a method developed by encryption teams at France Telecom, based on AES and OMAC, one candidate to replace SHA-1 and MD5, already proposed for Wi-Max. These protocols and authentication methods involve more and more powerful cards. "It took 30s to run TLS a year ago, now we're at 9s, soon it will be 5," Urien promised.■