Data Breaches and Security Bugs Drive Digital Certificate and Technology Interest

Contributed by Frost & Sullivan
Wednesday, 23 July 2014

The surge in the number of data breaches and recent security bugs such as Heartbleed has generated strong interest in digital certificates and technologies, including secure sockets layer (SSL) and public key infrastructure (PKI). PKI, in particular, remains the trusted technology for all projects where secured identity management is crucial.

New analysis from Frost & Sullivan, Global Certificates Marketsâ€"A Focus on Public Key Infrastructure, finds that the market earned revenues of $357.4 million in 2013 and estimates this to reach $532.8 million in 2017. The government sector is expected to account for the largest share of the total revenue owing to the implementation of several identity document projects.

The explosion of mobile devices, leading to the emergence of new usage models and habits, will further highlight the need to identify people, devices, and transactions, spurring the demand for PKI.

"In the past, many organisations saw very little benefit in employing PKI due to the lack of compatible applications, while enterprises and governments that used PKI encountered several problems within the system," said Frost & Sullivan Information and Communication Technologies Global Programme Director Jean-NoÃ«l Georges. "Today, the quality of PKI platforms and associated services has drastically improved, widening market potential."

While immense growth opportunities exist in the global market, the availability of newer secure solutions reduces the scope for PKI adoption. In addition, not all middleware require strong authentication.

The change management strategies necessary for such installations add to end-user reticence. To gain clients, providing a complete return on investment analysis that also takes into account the hidden costs of certificate management, profile lifetime, and form factor support is important.

"Companies and governments seek solutions that are flexible enough to work with existing systems and evolve to add new services or uses quickly and cost-effectively," stated Georges. "Certificate providers capable of supporting many devices, security requirements, usages, and systems to deliver a technology agnostic platform for certificate management will strengthen their position in the global PKI domain."