Press Release

# Elliptic Curve Cryptography "Made in Germany"

***[Essen, 25 June 2014]*** **Elliptic curves are mathematical structures that are being increasingly used in cryptographic methods. Together with the German Federal Office for Information Security (BSI), secunet has successfully pushed for the inclusion of new elliptic curves in international standards. As a result, the "Brainpool curves" created by the German ECC Brainpool working group can now be used in the encryption protocols TLS (Transport Layer Security) and IPSec (Internet Protocol Security).**

Beside RSA, Elliptic Curve Cryptography (ECC) is the most important class of asymmetric cryptosystems. One of the benefits of ECC compared to RSA is that considerably shorter keys can be used to achieve the same level of security. This has also an effect on the computational performance when encryption is used, for example, on mobile and other constrained devices.

However, the security provided by ECC heavily depends on the public parameters used, e.g. the coefficients of the curve. Since verification that a curve is indeed secure and suitable for use in cryptography takes a great deal of time and effort, typically, standardised parameters are used, for which these checks have already been carried out. The use of standardised parameters also simplifies the interoperability between different products.

Until now, only curves defined by the US standards institute NIST could be used in network protocols. However, the process by which these curves have been generated is not completely transparent. In the context of recent revelations on alleged back doors in cryptographic standards, this has led to considerable criticism. In contrast, the Brainpool curves created in 2005 by the German ECC Brainpool working group were derived directly from Pi and from Euler's number e. Derivation from the two most widely known natural constants ensures

# Press Release

maximum transparency and therefore guarantees a high degree of trust from users.

The Brainpool curves are already being put to use in German personal documents (new ID cards and passports) and in secunet's SINA encryption devices. In future, they will be used increasingly to secure public infrastructures, such as in smart meters in intelligent electricity grids or in healthcare.

In order to ensure that the Brainpool curves can also be used with TLS and IPSec, the corresponding standards of the Internet Engineering Task Force (IETF) had to be extended. secunet has successfully initiated and accompanied this standardisation process on behalf of the BSI. As a result, these communication protocols can now be used with elliptic curves that have been generated in a fully transparent manner, leaving no room for suspicions of back doors.

Number of characters: 2,734

**Press contact**

Christine Skropke
Spokesperson

Patrick Franitza
Dep. Spokesperson

secunet Security Networks AG
Kronprinzenstrasse 30
45128 Essen/Germany
Phone +49 201 54 54-1234
Fax +49 201 54 54-1235
E-mail: presse@secunet.com
http://www.secunet.com

**About secunet**

secunet is one of the leading German providers of high-quality IT security. Over 300 experts work in the areas of cryptography, e-government, business security and automotive security, and develop innovative products in these fields in addition to highly secure and reliable solutions. Many DAX companies as well as numerous authorities and organisations are among secunet's national and international customers, which total over 500. secunet is IT security partner of the Federal Republic of Germany and partner in the Alliance for Cyber Security.
secunet was founded in 1997 and achieved sales of EUR 63.9 million in 2013. secunet Security Networks AG is listed on the Prime Standard of the German Stock Exchange

*Additional data is available from www.secunet.com*