PKI PROVED TO BE A PROCESS NOT A TECHNOLOGY

Submitted by: Banner Corporation plc
Tuesday, 27 March 2001

Was it a lack of appropriate authentication processes or a failure to apply such processes that resulted in the recent Verisign and Microsoft certificate failure?

27th March, 2001 – Verisign has finally proved, beyond doubt, that Public Key Infrastructure (PKI) is not a technology, according to PKI consultancy and vendor De La Rue InterClear. After failing either to implement or follow appropriate authentication procedures to confirm identity, Verisign issued two Microsoft branded software publishing digital certificates to an impostor in January 2001. The system as a whole failed, leading to the realisation that technology alone will not offer effective protection from attempted fraud. In addition, it took almost two months to revoke the certificates. This is further compounded as users have no tools with which to check certificate status – can they be trusted?

As a result, from 29 January 2001 to 21 March 2001, users of Microsoft Windows 95, 98, NT, 2000 and ME have been at risk of using code that may have appeared to come from Microsoft, but which could actually have been corrupt code or even a virus, designed for fraudulent or malicious purpose. This problem persists as long as users do not, or are unable, to reliably check downloaded Microsoft software.

"The bottom line is that having the most robust encryption technology is irrelevant unless the authentication processes are applicable and implemented," commented Simon Bailey, business development director at De La Rue's online security arm, InterClear.

"If you give your house keys to a complete stranger, you'd count yourself lucky not to get burgled, but that doesn't make your keys the problem," he continued. " But why would a business give its 'keys' to a third party? After all, who knows who are the contacts, customers, partners and suppliers a business has relationships with? The business, or a third party?"

Who is best placed to determine the fundamental rules and processes by which trust is attributed? Why would organisations allow a third party to make such commercially sensitive decisions? Are independent third parties really able to authenticate genuine digital certificate applicants? Is it appropriate to give this level of control to an external organisation? The complete misconception that PKI is a technology solution is often the reason behind a company's decision to involve a third party.

A certificate server is a technology that can be used to generate digital certificates for anyone - regardless of whether the identity of the applicant is genuine or not. However, this is not where the security lies or where the trust values are delivered.

"PKI services rely on the identification and application of appropriate, and reliable authentication processes prior to certificate issuance and revocation. The risk of giving a third party the responsibility to determine these rules and processes is evident from this story," Bailey said. "At InterClear, we run the technology, and we will advise on how to put appropriate authentication procedures in place, but the rules governing who can be included in a trust network remain with the people who will suffer most if trust in the business is damaged – the client organisation itself."

De La Rue InterClear

InterClear – A De La Rue Company – was established in 1997 as the UK's first commercial digital Certification Authority (CA) to provide digital certificates authenticating individuals and companies using the Internet/Intranet/Extranet for transactions.
De La Rue InterClear designs, builds and maintains outsourced trust networks that provide identity proof and authentication to manage and reduce the legal, brand and technical risks of exploiting digital technologies.

InterClear enables companies to benefit from a PKI free from the financial and managerial burden of an in-house PKI, which demands the company to issue and manage its own certificates, and without the loss of control of an 'open' PKI solution that is based on third-party branded certificates often supplied by national utilities relying on inflexible technology, rules and regulations.
InterClear is a wholly owned subsidiary of De La Rue Plc (www.delarue.com) – the world's largest commercial security printer and papermaker, involved in the production of over 150 national currencies.

Media Contacts:

Debby Penton/Dawn Harnetty

Banner PR

tel: 020 7349 2200

email: interclear@b1.com

Simon Lofthouse

De La Rue InterClear

tel: 01256 487 700

slofthouse@interclear.com