Trust in real time for secure digital certificates

July 28 2006

CertiVeR, a European research project under the eTEN programme, developed and launched a complete and decentralised service for certification authorities (CAs) and other users. The technology – a secure online certificate status information system – has resulted in a high performance, flexible service available 24/7 that validates and revokes digital certificates in real time.

"Now, users can be sure that the digital credential is secure and valid," explains Oscar Manso. "A digital certificate is like a passport. If it is stolen, it can be reported and cancelled, or revoked."

CertiVeR offers a certificate validation and revocation service with the corresponding Online Certificate Status Protocol (OCSP) publication. This enables the user to verify the state of a specific certificate before

executing any operation or transaction upon it. The system is available to any certificate authority in the world, but the consortium is focusing on Europe where the e-Signature Directive requires the provision of this service across all EU Member States.

The use of electronic signatures requires the verification of the signature policy, which includes the validation of all the certificates in the signer's certification path. However, as Manso explains, the time between when a certificate may have been revoked and the time the new Certificate Revocation List (CRL) is released, could be significant.

A CRL is a list of certificates and their serial numbers that have been revoked, are no longer valid and should not be relied upon by any system user. For example, a certificate is revoked if the CA had improperly issued a certificate or if a private key is believed to be compromised. In the past, CAs did not use an online validation service, resulting in delays of up to one week.

"Because CertiVeR operates in real time, this security barrier is overcome," he says. "CertiVeR can be connected to all CAs in Europe to refresh the status of certificates. Users can now have a single access point. Certificate revocation is easier and safer, which increases transaction confidence, and there is now a single phone number to revoke all certificates."

CAs, both private and public, would profit from CertiVeR's real time information. This level of service is far too complex and expensive to be run individually. Cost savings are realised as a result of the technical, managerial and R&D economies of scale.

CertiVeR establishes secure connection interfaces with the CAs to obtain identification information about a user. Several identification systems can be used to identify CA users, including voice biometrics.

When a user wants to revoke a certificate, a call is made to the central revocation number. The automated call centre system tries to verify the identity of the caller through voice recognition technologies.

If the automated system is unable to verify the call, it is transferred to an operator who tries to determine the user's identity by means of secret questions and general information stored. Once a user is validated into the certificate revocation system, the user can suspend or activate any certificates in real time.

CertiVeR's online certification status information system was originally developed to fill the needs of the financial sector. A secure central repository for certificate revocation information creates and manages revocation documents and authenticates requests following the requirements of the ISO 10779 standard.

Twelve pilots at European and global level include three currently running that, according to Manso, are performing "very well". A significant pilot ran with TERENA (Trans European Research and Education Networking Association) in The Netherlands. In this instance, the consortium created TACAR, TERENA's Academic CA Repository, and worked on getting the appropriate root CA certificates needed by users' browsers in a practical and cost-effective manner.

CertiVeR also participated in the production of open source tools and demo environments to promote the adoption of real-time validation environments at global level. The consortium is now targeting software developers to simplify the validation so they can create applications with a single point of access.

"Other end users can take advantage of CertiVeR's infrastructure to validate and use their digital signatures for activities such as electronic bills and online transactions," he adds. "The potential for B2B and B2C

applications is huge."

Manso expects a full-scale marketing effort to be launched this October.

Source: IST Results