authors D. Berbecaru, A. Desai, A. Lioy

title A unified and flexible solution for integrating CRL and OCSP into PKI applications

journal Software: Practice and Experience

ISSN 0038-0644

issue Vol. 39, Issue 10, July 2009

pages 891-921

DOI 10.1002/spe.918

abstract Public key certificates (PKCs) are used nowadays in several security protocols and applications, so as to secure data exchange via transport layer security channels, or to protect data at the application level by means of digital signatures. However, many security applications often fail to manage properly the PKCs, in particular when checking their validity status. These failures are partly due to the lack of experience (or training) of the users who configure these applications or protocols, and partly due to the scarce support offered by some common cryptographic libraries to the application developers.

This paper describes the design and implementation of a light middleware dealing with certificate validation in a unified way. Our middleware exploits on one side the libraries that have already been defined or implemented for certificate validation, and it constructs a thin layer, which provides flexibility and security features to the upper layer applications. In our current approach, this layer boasts an integrated approach to support various certificate revocation mechanisms, it protects the applications from some common security attacks, and offers several configuration and performance options to the programmers and to the end users. We describe the architecture of this approach as well as its practical implementation in the form of a library based on the famous OpenSSL security library, and that can be easily integrated with other certificate-aware security applications.