A straightforward method for creating and verifying digital signatures in HTML forms

R. Palacios Hielscher; D. de la Fuente González

Abstract-

Web-based forms, created in HTML language, are widely used to submit data to Internet servers. However the process of submitting forms using http protocol is anonymous. In this article, two pieces of code are provided to add digital signature to standard html forms in a simple way. The first code is a JavaScript function (signForm) that can be included into any HTML page containing a form. The function must be called upon submission so it can generate a digital signature that will be sent over the Internet along with the form data. The second piece of code is a PHP function (Validation) to be included in the program that usually checks form data and stores the values in a database. The presented function will automatically verify the digital signature by concatenating form values in the same way as it was done in the Javascript function, and finally calling openssl for PKCS7 digital signature verification. In addition, some helpful PHP functions are also included to make it easy, for a programmer not very familiar with cryptography, to extract internal data from the digital certificate. By using the provided functions, any current process can easily incorporate digital signature just by adding a piece of JavaScript code to the existing forms and another piece of code to the server-side PHP program in charge of processing uploaded data.

Index Terms- http://www.drdobbs.com/web-development/212701413

Due to copyright restriction we cannot distribute this content on the web. However, clicking on the next link, authors will be able to distribute to you the full version of the paper:
Request full paper to the authors

If you institution has a electronic subscription to Dr Dobbs Journal (on-line), you can download the paper from the journal website:
Access to the Journal website

Citation:
Palacios, R.; de la Fuente, D. "A straightforward method for creating and verifying digital signatures in HTML forms", Dr Dobbs Journal (on-line), no.417, pp.1-36, January, 2009.