

## Avoco Secure secure2signHTML

### Summary

secure2signHTML is a control for zero footprint, client-side digital signing of HTML (web) forms.

It produces a standard PKCS#7 format signature, which is returned with the form data when the form is submitted. The signature can be subsequently verified using existing tools, or using the secure2signHTML verifier.

Because the appearance, or text, of the form web page could be changed dynamically, using style sheets or scripts, a screen capture of the web page at the time of signing is included in the signature. Also included is a time stamp from an authorised time source to RFC 3161, ensuring that the signing time is recorded from a cryptographically secure source.

Importantly, the certificate used for signing is validated at the time of signing, and if a third party OCSP client (such as Tumbleweed or CoreStreet) is installed, the log of the certificate validation is stored in the signature for audit purposes.

The control (small, at around 100 k) is simple to add to any web page that has standard <FORM> elements; it offers a range of configuration options (*e.g.* to restrict certificate selection to those with specific policies, issued by specific Certificate Authorities or issued to a specific individual, *etc.*) through scripting or <param> statements on the page.

On signing, the PKCS#7 signature is saved locally, and after base64 encoding is also returned in a hidden field on the form; in this way the signature is returned with the other form data when the form is submitted.

For details and advice on using secure2signHTML in your organisation, please contact either:

[info@avocosecure.com](mailto:info@avocosecure.com) or [sales@avocosecure.com](mailto:sales@avocosecure.com)

 [info@avocosecure.com](mailto:info@avocosecure.com)

US: +1 415 839 9433

International: +44 207 851 6070

 [www.avocosecure.com](http://www.avocosecure.com)

Copyright © Avoco Secure Ltd 2008