152297

GAO United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-258013

August 11, 1994

Anthony R. Torrice
Chief Disbursing Officer
Financial Management Service
Department of the Treasury

Dear Mr. Torrice:

In your letter of May 5, 1994, you requested our views on whether the Department of the Treasury could rely on a combination of a secure hash value and message authentication code to perform the electronic signature requirements for a certifying officer. As discussed below, we believe such a concept can provide an acceptable method for a certifying officer to certify payments.

Based on the information contained in your letter and discussions with your staff, Treasury is proposing to have an agency generate a hash value on its payment information. This hash value will be computed using the algorithm outlined in the Secure Hash Standard[1] (Federal Information Processing Standard 180). The hash value will then be electronically signed by the certifying officer using a message authentication code generated in accordance with the procedures in your current Electronic Certification System. We sanctioned your current system in November 1988.

As we understand your proposal, Treasury will then receive the payment information, hash value, and the certifying officer's electronic signature from the agency. Treasury will recompute the hash value and ensure that it agrees with the value

[1] The Secure Hash Standard provides an algorithm designed so that it is computationally infeasible to (1) find a message which corresponds to a given hash value or (2) find two different messages which will produce the same hash value.

electronically signed by the certifying officer. It will complete the validation process by verifying the message authentication code generated by the certifying officer on the hash value. If these two validations are successful, the data can be considered unchanged and accepted by Treasury for further processing.

We believe that properly combining a hash value and a message authentication code can generate electronic signatures that provide at least the same quality of evidence as the handwritten signatures they are designed to replace. Specifically, this concept can generate a signature that is (1) unique to the signer, (2) under the signer's sole control, and (3) capable of being verified by the recipient.[2] In addition, the signature would be generated in a manner that links it to the data so that any changes in the data after the certifying officer has generated the electronic signature will be detected by the validation process.

This letter only addresses your concept and does not sanction Treasury's planned electronic signature system that will use this method. It also does not constitute GAO approval of your financial management system, as defined by 31 U.S.C. 3512(f)(2).

We look forward to working with Treasury on this and other efforts in the future. Should you have any questions, please contact Chris Martin of my staff at (202) 512-9481.

Sincerely yours,

Rona B. Stillman
Chief Scientist
Computers and Communications

(511472)

[2] We have outlined, generally, the necessary attributes of electronic signatures in Comptroller General decision 71 Comp. Gen. 109 (1991).