normally will be made available within 60 days of the filing of the petition. The deadline for submission of comments on the EA will generally be within 30 days of its service.

Board decisions and notices are available on our website at WWW.STB.DOT.GOV.''

Decided: December 22, 2000.

By the Board, David M. Konschnik, Director, Office of Proceedings.

Vernon A. Williams,

Secretary.

[FR Doc. 01–27 Filed 1–2–01; 8:45 am]

BILLING CODE 4915–00–P

DEPARTMENT OF THE TREASURY

Fiscal Service

Electronic Authentication Policy

AGENCY: Financial Management Service, Fiscal Service, Treasury.

ACTION: Notice of publication of policies and practices for the use of electronic transactions and authentication techniques in Federal payments and collections.

SUMMARY: The Office of Management and Budget (OMB), as part of its procedures to implement the Government Paperwork Elimination Act (GPEA), directed the Department of the Treasury (Treasury) to develop, in consultation with Federal agencies and OMB, policies and practices for the use of electronic transactions and authentication techniques in Federal financial transactions, including payments and collections. In accord with this directive, Treasury is publishing this Electronic Authentication Policy.

FOR FURTHER INFORMATION CONTACT: Gary Grippo, Director, Electronic Commerce, Financial Management Service, Department of the Treasury, 401 14th Street, S.W., Washington, DC 20227, (202) 874–6816, gary.grippo@fms.treas.gov.

SUPPLEMENTARY INFORMATION: The Government Paperwork Elimination Act (GPEA), Public Law 105–227, Title XVII, was signed into law on October 21, 1998. GPEA requires Federal agencies to allow individuals and entities, when practicable, the option of submitting information to or transacting business with the agency by electronic means. On May 2, 2000, the Office of Management and Budget (OMB) issued procedures and guidelines for the implementation of the Act. 65 FR 25508. That guidance directed the Department of the Treasury (Treasury) to develop policies and practices to be followed by agencies when making Federal payments and collections electronically, as well as other financial transactions. In particular, Treasury was directed to address the authentication of the identity of parties to such transactions, in furtherance of the goals of GPEA in these policies and practices.

Pursuant to this directive, on March 15, 2000, Treasury forwarded to OMB for circulation among Government agencies a draft policy document outlining the principles and guidelines for the use of electronic authentication techniques for Federal payment, collection and collateral transactions. In response to comments received from Government agencies on the draft policy document, Treasury has revised the guidance accordingly. The final policy document is reproduced below.

The most current version of the policy may be found on the Financial Management Service website at: http://www.fms.treas.gov/eauth/index.html. Given the rapidly changing nature of electronic commerce, electronic authentication techniques and the related technology infrastructure, Treasury views this policy guidance as a dynamic document which may be revised as necessary, and will accept comments at any time. Changes to this policy will be published as Notices in the **Federal Register**, as necessary, and posted to the FMS website.

Electronic Authentication Policy Payment, Collection, and Collateral Transactions

Background Discussion

Purpose: This policy sets forth principles on the use of electronic authentication techniques, including digital signatures, for Federal payment, collection, and collateral transactions conducted over open networks such as the Internet. Federal payment and collection transactions include all transactions intended to effect a credit or a debit to an account, including transactions executed by Non-Treasury Disbursing Offices. Federal collateral transactions include all electronic messages or instructions to pledge, deposit, release, or claim collateral used to secure public funds. These payment, collection, and collateral transactions may be between the Federal Government and non-Federal entities, as well as transactions between Federal entities.

Scope: This policy applies to applications that use open networks, including the Internet, since access to these networks is unrestricted and Federal users and trading partners must be authenticated accordingly. This policy is not intended to apply to transactions over closed networks, *i.e.,* legacy financial networks where the networking infrastructure and access to it is owned or controlled by the Government, the Federal Reserve, or private financial institutions.

Focus is also placed on the use of public key cryptographic techniques, which can provide for robust electronic authentication, and on the manner in which Federal agencies must go about obtaining public key digital certificates for payment, collection, and collateral transactions. (It should be noted that in establishing such guidance, our intent is not necessarily to dictate that a particular certification authority provider be used, but rather to try to follow a general principle that offers agencies some choice, particularly where commercial certification authorities must be relied upon). In addition to public key cryptography, the policy covers other forms of remote electronic authentication and electronic signatures, including but not limited to knowledge-based authentication (Personal Identification Numbers (PINs) and passwords) and biometrics.

Goals of Authentication. The goals of authentication are to protect the integrity of Federal payment, collection, and collateral transactions by (1) ensuring that transactions are conducted only by authorized individuals, (2) pinpointing accountability and liability for transactions, (3) providing assurances to the public about the identity of Federal servers and systems on open networks, and (4) receiving assurances about the identity of commercial servers and systems on open networks. The different electronic authentication techniques achieve these goals with varying degrees of robustness.

In addition, the use of the Internet with appropriate electronic authentication techniques offers new opportunities to expand the use of the payments system. For example, digital signatures may allow finance officers to authorize Automated Clearing House (ACH) and wire transfer payments on-line, permitting the end users access to otherwise closed bank payment networks. These techniques will also permit electronic payments to be made peer-to-peer for the first time, using mechanisms such as electronic checks and electronic cash.

Techniques. Electronic authentication techniques include, but are not limited to, the following:

- Knowledge based authentication, or shared secrets, such as PINs and passwords;

• Biometrics, such as fingerprint, voice, and eye characteristics;
• Secure tokens, such as smart cards;
• Cryptography, including digital signatures, challenge-response protocols (*e.g.,* the ''handshake'' protocol in Secure Sockets Layer), and message authentication codes;
• Digitized signatures, including digital images of handwritten signatures and signature dynamics (*i.e.,* measurements of the direction, pressure, speed, and other attributes of a handwritten signature).

These electronic authentication techniques provide varying levels of security and non-repudiation. In practice, however, a robust authentication system will make use of multiple techniques in combination, such as the use of a PIN to unlock and apply a digital signature private key held on a smart card. While the scope of this policy is limited to payment, collection, and collateral transactions, these techniques may be applied to other types of financial transactions conducted over open networks, such as secure remote access to financial systems, and transmission of accounting data.

Finally, it is important to note that the policy sets forth a model for determining the robustness of electronic authentication for particular types of transactions, but does not generally dictate that a specific technique or system be used. (The lone exception to this approach is a requirement for public key digital signatures for transactions determined to be in the high risk category.) In this sense, the document is limited to policy guidance, and does not address specific constructs for implementing electronic authentication techniques or supporting their interoperability, such as the potential use of the Federal Bridge Certification Authority in support of interoperating public key infrastructures, or the use of the BioAPI specification for biometric implementations. We recognize, however, that as authentication mechanisms and the ways in which they interoperate mature, it may be appropriate to incorporate additional guidance into the policy. The policy will be updated as necessary as such matters develop.

Electronic Authentication Techniques for Federal Payment, Collection, and Collateral Transactions

Section 1. Title

Use of Electronic Authentication Techniques for Federal Payment, Collection, and Collateral Transactions

Section 2. Scope

This policy applies to all Federal payment, collection, and collateral transactions, as defined herein, conducted over open networks such as the Internet, including those transactions executed by statutory Non-Treasury Disbursing Offices (NTDO) and delegated NTDOs.

Section 3. Definitions

(a) *Banking industry standards* means standards promulgated by the X9 Accredited Standards Committee for Financial Services.

(b) *Certificate* means a secure digital document that binds a public cryptographic key to a person (or organization) in order to provide a measure of proof that the person is who he or she claims to be in a transaction.

(c) *Certification authority* means an entity trusted to issue digital certificates.

(d) *Collateral transaction* means any message, instruction, request, or authorization that is intended to pledge, deposit, move, release, claim, or otherwise manage collateral used to secure public funds.

(e) *Collection* means a transaction entry, object, or instruction, or a transaction request or authorization, that is intended to effect a credit of funds to the Treasury, an account at a Treasury designated depositary, or any other account holding public funds.

(f) *Cryptographic credential* means an electronic document or object containing a cryptographic key which provides evidence of authority to conduct a transaction and/or provides assurance that a system or person is what or who it claims to be. A public key digital certificate is an example of a cryptographic credential.

(g) *Delegated NTDO* means a Non-Treasury Disbursing Office whose authority to disburse public funds has been delegated at the discretion of the Treasury.

(h) *Federal standards* means Federal Information Processing Standards (FIPS) promulgated by the National Institute of Standards and Technology (NIST) and standards promulgated by the Treasury Department.

(i) *Financial agent* means a commercial financial institution designated by the Treasury to act as a depositary of public money or financial agent of the Government, under the provisions of 31 CFR 202 and 203.

(j) *Fiscal agent* means a Federal Reserve Bank designated by the Treasury to act as a Government depositary or fiscal agent.

(k) *Payment* means a transaction entry, object, or instruction, or a transaction request or authorization, that is intended to effect a debit of funds against the Treasury, an account at a Treasury designated depositary, or any other account holding public funds.

(l) *Statutory NTDO* means a Non-Treasury Disbursing Office whose authority to disburse public funds is established by statute.

(m) *Trading partner* means any individual, business, organization, or governmental entity that receives funds or collateral from, or sends funds or collateral to, the Federal Government.

Section 4. General Principles

(a) The Secretary of the Treasury is responsible for promulgating governmentwide policies and practices on the use of electronic authentication techniques, including techniques that rely on public key certificates and other cryptographic credentials, to secure payment, collection, and collateral transactions.

(b) *Financial agents.* All financial agents of the Treasury which use cryptographic authentication in the conduct of Government fiscal operations shall obtain their cryptographic credentials, including certification authority credentials, from the Treasury or, at the discretion of the Treasury, from a fiscal agent.

Example: A commercial bank is designated to operate a new cash concentration system for the Treasury, which will collect funds from various receipt accounts and deposit them into the Treasury. The bank sets up a certification authority to issue certificates to the holders of the receipt accounts so that they can use the Internet to authorize the concentration of their receipts. This bank certification authority would operate under a Treasury ''root'' certification authority. The Treasury root certification authority would issue a single certificate validating the agent bank certification authority and the bank's status as a designated agent of the Treasury. The agent bank certification authority would in turn issue the end user certificates.

(c) *Fiscal agents.* Fiscal agents that use cryptographic authentication in the conduct of Government fiscal operations shall obtain their cryptographic credentials, including certification authority credentials, from the Treasury or, at the discretion of the Treasury, shall create and use their own cryptographic credentials.

(d) *NTDOs.* All delegated NTDOs that use cryptographic authentication in the issuance of Federal payments shall obtain their cryptographic credentials, including certification authority credentials, from the Treasury. Certification authority credentials may be granted in the form of a subsidiary certification authority certificate, a cross-certificate, or otherwise.

Consistent with this provision, delegated NTDOs may issue end user public key certificates. Statutory NTDOs which use cryptographic authentication in the issuance of Federal payments may create and use their own cryptographic credentials, in accordance with all other provisions of this policy.

(e) All electronic authentication techniques used in support of Federal payment, collection, and collateral transactions must be based on either Federal standards or banking industry standards. To the extent that Federal or banking industry standards are absent, the Treasury may approve the use of other voluntary consensus body standards.

(f) Nothing in this policy is intended to relieve a Federal agency of its responsibility to comply with other Federal systems security guidelines, including OMB Circulars and Federal Information Processing Standards, or to implement appropriate Internet security mechanisms, such as firewalls and intrusion detection programs.

(g) The Fiscal Service of the Treasury, acting on behalf of the Secretary of the Treasury, is responsible for implementing and interpreting this policy.

Section 5. Risk Model

(a) All payment, collection, and collateral transactions must be properly authenticated, in a manner commensurate with the risks of the transaction. For any given Federal agency cash flow or program (*e.g.,* corporate user fees, benefit payments, excise taxes, retail product sales, investment collateral, etc.) Federal agencies shall assess overall risk and determine the appropriate electronic authentication technique in accordance with the following risk model.

(1) The three general factors used to determine the overall risk of Federal payment, collection, and collateral transactions are: risk of monetary loss, reputation risk, and productivity risk.

(2) The risk of monetary loss is determined using a variety of elements, including but not limited to:

(A) Average dollar value of transactions.

(B) Loss to the Government.

(C) Loss to a consumer.

(D) Loss to a business, state or local government, or other trading partner.

(E) Rules for reversing and repudiating a transaction (*e.g.,* in the Uniform Commercial Code, the ACH rules, the Code of Federal Regulations, Federal Reserve regulations, Generally Accepted Accounting Principles, or bank network operating procedures).

(F) Body of law applied to the transaction.

(G) Liability for the transaction (*e.g.,* personal, corporate, insured, or shared).

(3) The reputation risk to the Government in the event of a breach or an improper transaction is determined using elements such as:

(A) Relationship with the trading partner (*e.g.,* debiting a consumer account vs. intragovernmental payment between Federal agencies, and voluntary vs. mandatory transactions).

(B) Public visibility and public perception of programs.

(C) History or patterns of problems or abuses.

(D) Consequences of a breach or improper transaction (*e.g.,* normal exception handling vs. imposition of penalties).

(4) Productivity risk associated with a breach or improper transaction is determined using elements such as:

(A) Time criticality of transactions (*e.g.,* entitlement payment vs. contractor payment).

(B) Scope of system and number of transactions (*e.g.,* national or governmentwide system vs. localized system).

(C) Number of system users or dependents.

(D) Backup and recovery procedures.

(E) Claims and dispute resolution procedures.

(b) Assessing the combined risk factors (monetary loss, reputation risk, and productivity risk) determines the risk category of a cash flow, program, or system. For purposes of Federal payment, collection, and collateral transactions, there are four risk categories: high, moderate, low, and negligible. The risk category indicates the robustness of the electronic authentication technique that must be used. Authentication rules for each of the risk categories are listed below. High and moderate risk transactions require multi-factor authentication, where at least two electronic authentication techniques must be used in combination, such as digital signature with a PIN protecting the signing key.

(1) *High Risk.*

(A) Multi-factor authentication is required, including a digital signature.

(B) Private cryptographic keys must be generated, stored, and used in a secure cryptographic hardware module.

(C) Certification authorities must operate under the Government's direct policy authority.

(2) *Moderate Risk.*

(A) Multi-factor authentication is required.

(B) Private cryptographic keys may be stored in software.

(C) Certification authorities which are under the policy authority of a commercial entity meeting the requirements of this policy may be used.

(3) *Low Risk.* Single factor authentication must be used, such as a PIN or a software based SSL client certificate.

(4) *Negligible Risk.* Transactions may occur without an electronic authentication technique.

(c) Federal agencies must apply the risk categories, determined using the three risk factors, to all payment, collection, and collateral transactions using open networks.

(d) In determining risk categories, Federal agencies should take into account programmatic controls which mitigate the intrinsic risks of conducting transactions over an open network. (For example, a consumer who submits an Internet payment for goods in a Government auction may have to appear in person with identification to retrieve the goods. This may argue for a lower category of risk for the Internet transaction.)

(e) The risk category determined for a set of transactions represents the minimum security required. Federal agencies may apply the requirements of a higher risk category, or a stronger authentication technique, at their option. Agencies should contact Mr. Gary Grippo of the Financial Management Service, (202) 874–6816, gary.grippo@fms.treas.gov, with any questions about the application of this risk-based model.

Section 6. Collections Policies

(a) Federal collections systems and servers that cryptographically authenticate themselves to Federal trading partners during financial transactions must receive their cryptographic credentials from or through the Treasury or the Treasury Financial agent that processes the collection.

Example: An agency sets up a Web site to receive credit card numbers for the payment of fines. A public key certificate on the Web server provides citizens with an assurance that the collection Web site is operated by the Federal Government. Since this is a credit card collection, the agency would obtain its server certificate from one of the Financial Management Service's designated financial agent banks that processes credit cards and makes available to the agency certificates from one or more commercial or government certificate authorities. This financial agent bank is the entity sponsoring the agency into the credit card system and is liable for the agency's transactions.

(b) Federal collections systems and servers that cryptographically authenticate themselves to Federal

trading partners during financial transactions must generate, store, and use their private cryptographic keys in a secure cryptographic hardware module.

(c) In processing collection transactions from Federal trading partners that have a risk category other than ''Negligible,'' Federal agencies shall only trust cryptographic credentials issued or honored by the institution that maintains the trading partner's transaction account, or issued by a Federal agency.

Example: A small business goes to a Federal Web site to enroll in a repayment program for a Federal loan. The business digitally signs an electronic form indicating that the Federal agency may initiate ACH debits against its bank account to repay the loan, and then transmits the signed form along with its certificate to the Federal agency. The Federal agency determines that the certificate was issued by an independent commercial certification authority. The Federal agency rejects the enrollment under this policy, because the certification authority has no connection to the consumer's banking relationship.

Dated: December 22, 2000.

Kenneth R. Papaj,

Acting Commissioner, Financial Management Service.

[FR Doc. 01–79 Filed 1–2–01; 8:45 am]

BILLING CODE 4810–35–P

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

Submission for OMB Review; Comment Request

December 28, 2000.

The Office of Thrift Supervision (OTS) has submitted the following public information collection requirement(s) to OMB for review and clearance under the Paperwork Reduction Act of 1995, Public Law 104–13. Interested persons may obtain copies of the submission(s) by calling the OTS Clearance Officer listed. Send comments regarding this information collection to the OMB reviewer listed and to the OTS Clearance Officer, Office of Thrift Supervision, 1700 G Street, NW., Washington, DC 20552.

DATES: Submit written comments on or before February 2, 2001.

OMB Number: 1550–0059.

Form Number: OTS Form 1583.

Type of Review: Regular.

Title: Capital Distribution.

Description: Provides uniform treatment for capital distributions made by savings associations held by holding companies. Ensures adequate supervision of distribution of capital by those savings associations, thereby fostering safety and soundness of the thrift industry.

Respondents: Savings and Loan Associations and Savings Banks.

Estimated Number of Responses: 687.

Estimated Burden Hours Per Response: 4 hours.

Frequency of Response: Once per occurrence.

Estimated Total Reporting Burden: 2,748 hours.

Clearance Officer: Ralph E. Maxwell, (202) 906–7740, Office of Thrift Supervision, 1700 Street, NW., Washington, DC 20552.

OMB Reviewer: Alexander Hunt, (202) 395–7860, Office of Management and Budget, Room 10202, New Executive Office Building, Washington, DC 20503.

John E. Werner,

Director, Information & Management Services.

[FR Doc. 01–123 Filed 1–2–01; 8:45 am]

BILLING CODE 6720–01–P