NR 98-4
January 13, 1998

OCC APPROVES A NATIONAL BANK TO CERTIFY DIGITAL SIGNATURES

Washington, D.C. -- The Office of the Comptroller of the Currency (OCC) has conditionally approved an application for a Utah bank to be the first financial institution to offer digital signature products to its customers. Digital signatures are used for electronic authentication of the sender of an electronic message -- much like a notary verifies the signature of an individual in a physical setting. As interest grows in electronic commerce, digital signatures can provide an important way for consumers and businesses to decide which electronic communications they can trust.

The approval permits Zions First National Bank, Salt Lake City, Utah, to establish an operating subsidiary to act as a certification authority to enable subscribers to generate digital signatures that verify the identity of a sender of an electronic message. The certificate process will also enable subscribers to be certain that communications received have not been altered during transmission.

"The ability to verify and authenticate electronic signatures is essential to the development of electronic commerce and electronic banking," said Comptroller of the Currency Eugene Ludwig. "Banks, which have long played a role as trusted intermediaries in financial transactions, are ideally situated to provide this type of service."

The bank plans initially to support the transmission and authentication of electronic filings by attorneys dealing with the Utah court system.

The bank plans to focus on certification services primarily involving corporate and government contracts. The bank will provide advance notice to the OCC before it provides certification services directly to the public.

In connection with its application, the subsidiary has committed to provide consumer protection, including clear and appropriate consumer disclosures on issues relating to general rights and responsibilities, as well as privacy, error resolution procedures, and relevant fees.

As part of its ongoing supervision of the activity, the OCC expects the bank to implement and maintain a risk management system that identifies, measures, monitors, and controls the material risks of the activity. Accordingly, the OCC's approval is conditioned on the bank's submission of a final blueprint of its information system. The OCC also expects the bank, which is well capitalized and well managed, to maintain adequate capital to support this activity.

The operating subsidiary will have internal data-processing

systems that are year 2000- compliant, in accordance with OCC guidelines. It has committed to perform due diligence to ensure that third-party data-processing service providers or purchased applications or systems also will be year 2000-compliant.

The OCC concluded that the activity approved today is permissible, upon application, for national banks and their operating subsidiaries because it resembles verification and identification services, such as notary services, already performed by national banks and is, therefore, part of the business of banking. The activity does not involve provisions of the OCC's part 5 rule governing bank operating subsidiary activities that are different from activities permissible for parent national banks.

Attached is an explanation of how a digital signature system works.

How a Digital Signature System Works: A Simplified Example

Step 1: A person wishing to use digital signatures to authenticate electronic messages obtains either a pair of public and private signature keys or software that will generate a public/private key pair. The private key is used to encode (i.e., scramble) and the public key to decode (i.e., unscramble). The same person (now called a "subscriber") obtains a certificate from a certification authority that verifies the association between the subscriber and the public/private key pair. The certification authority publishes the subscriber's public key in the authority's electronic repository.

Step 2: The subscriber prepares an electronic message document file (e.g., a letter) and, then, an electronic "hash" of that message using a special hash function that is part of the digital signature program. The resulting "hash" is a relatively brief electronic file of characters and numbers that uniquely summarizes the "hashed" message so that any changes in the message would change the "hash" file.

Step 3: The subscriber encodes the hash file using the private key with another part of the digital signature program.

Step 4: The subscriber attaches the encoded hash file to the non-scrambled letter file and transmits both files to the recipient with a copy of the subscriber's digital certificate containing the subscriber's public key.

Step 5: The recipient makes a new electronic hash of the letter file received using the same hash program used by the sender. Also, using the subscriber's public key, the recipient decodes the encoded hash file received with the message. If needed, the recipient can confirm the subscriber's public key with the certification authority.

Step 6: If the sender's public key decodes successfully the encoded hash file, the recipient knows that the sender must have

authorized the sending of that file. Also, if the decoded hash file matches the hash file made from the attached letter file, the recipient knows that the letter was not altered during transmission. Thus, the digital signature system verifies both the source and the contents of the letter.

# # #

The OCC charters, regulates and supervises more than 2,600 national banks and 66 federal branches and agencies of foreign banks in the United States, accounting for 56 percent of the nation's banking assets.
Its mission is to ensure a safe, sound and competitive national banking system that supports the citizens, communities and economy of the United
States.