Appendix B

ANCILLARY SERVICES

Depending on the scope of transactions and messages for which subscribers use digital certificates, there are a number of other ancillary services that may be part of a CA system.

Private Key Escrow

Once the subscriber has requested or generated a public/private key pair for a digital certificate, each key requires different treatment. While the public key as certified by the CA will be made available for appropriate use by relying parties, the subscriber's private key necessarily is for his exclusive use. A subscriber will want easy access to additional copies of his private key, in case it is accidentally corrupted or deleted. The CA may provide escrow services as a backup for their subscribers. Such key escrow services create transaction and reputation risk exposures if the CA does not implement sufficient physical and logical security to limit unauthorized internal and external access to stored private keys.

Archival Services

In addition to the repository of valid certificates, subscribers and relying parties may have need for an archive of once-valid, but no longer active, digital certificates used for authenticating past transactions and messages. The risks involved with this function are the same as those for maintaining the integrity of any large data base, including transaction and reputation risk associated with managing access to the database.

Certificate Manufacturer

A CA issuer may outsource some technology operations to a certificate manufacturer. Banks may serve as a manufacturer for other entities that act as CA. Depending on the contract between the issuer and the manufacturer, the manufacturer is likely to generate the issuer's own public/private key pair. In addition the manufacturer may generate, sign, and publish subscriber certificates under direction of the issuer. The risks involved with this function are the strategic, reputation, and transactions risks associated with certificate issuance. The overall risk exposure would be shared between the certificate manufacturer and issuer, according to the terms of their contract.

Message Encryption

Some digital signature software includes an option to encrypt messages that are digitally signed. Although not necessary for message authentication, or for proof of data integrity, message encryption restricts access to messages and transactions to those persons who know the code. While a CA providing such software has the transaction and reputation risk exposures of any company providing a similar software product, its compliance risk exposure can be even more significant. This compliance risk arises from the uncertain legal environment and public policy

position with respect to encryption. There are restrictions on encryption export and an ongoing domestic debate about law enforcement access to encrypted information.

Time Stamping

Some documents require a specific time assigned to identification or validation. If the software application allows subscribers to insert a time stamp, the CA is exposed to additional transaction risk from the possibility that an incorrect time or date is assigned to a digitally signed document.