A **key escrow encryption system** (or, simply escrowed encryption system) is an encryption system with a backup decryption capability that allows authorized persons (users, officers of an organization, and government officials), under certain prescribed conditions, to decrypt ciphertext with the help of information supplied by one or more trusted parties who hold special data recovery keys. The data recovery keys are not normally the same as those used to encrypt and decrypt the data, but rather provide a means of determining the data encryption/decryption keys. The term *key escrow* is used to refer to the safeguarding of these data recovery keys. Other terms used include *key archive*, *key backup*, and *data recovery system*. [Since this paper was published, the term *key recovery* has also become commonplace. Another term that is used, particularly in Europe, is *Trusted Third Parties.*]"

-By Dennis K. Branstad and Dorothy E. Denning

**What's the use?**

With the key escrow system, authorized individuals, such as government and law enforcement officials, have access to the private key of email encryptions through a third party escrow service. This private key is only released by the third party when there is a just reason to do so. This system is important to implement in the highly advanced computer world of today—in which private information could be labeled as a public threat. The only way to examine this is through the key escrow system.

**Sources:** [http://www.cosc.georgetown.edu/~denning/crypto/Taxonomy.html](http://www.cosc.georgetown.edu/~denning/crypto/Taxonomy.html)