HMRC internal manual

Cryptoassets Manual

From: **HM Revenue & Customs (/government/organisations/hm-revenue-customs)**

Published: 30 March 2021

Updated: 28 November 2025 - **See all updates (/hmrc-internal-manuals/cryptoassets-manual/updates)**

CRYPTO10350 - Introduction to cryptoassets: public and private keys

Encryption keys are a vital aspect of cryptography. They make a message, transaction or data value unreadable for an unauthorised reader or recipient, so it can only be read and processed by the intended recipient.

Exchange tokens rely on a public and private key system:

- The private key is a randomly generated string and is used to authorise a transaction involving tokens held at a public address.
- A public key is mathematically generated from the private key, linking the two keys cryptographically.

For all practical purposes, a private key cannot be generated from a public key.

The public address is shared across the Distributed Ledger (DL). Anyone who knows that address can look at the DL and see all transactions to and from the public address. Any person who knows the public and private keys can authorise transactions involving tokens held at the relevant public address.

If a private key is lost, the tokens will continue to exist at the public address. However, the 'owner' would be unable to undertake any transactions in respect of those tokens. If private key details were kept only on a computer which was subsequently destroyed, then the tokens would be unreachable, although they would continue to exist.

← **Previous page**
(/hmrc-internal-manuals/cryptoassets-manual/crypto10300)

→ **Next page**
(/hmrc-internal-manuals/cryptoassets-manual/crypto10375)