RSA SecureID

Return to Glossary is a mechanism developed by RSA for performing Two-Factor Authentication (2FA) for a user to a network resource.

The **RSA SecurID** is an Authentication mechanism consisting of a “token”—either Hardware (H/W) (e.g. a key fob) or Software (SW) (a soft token)—which is assigned to a computer user and which creates an authentication code at fixed intervals (usually 60 seconds) using a built-in clock and the card's factory-encoded almost random key (known as the “seed”). The seed is different for each token, and is loaded into the corresponding **RSA SecurID** Server (RSA Authentication Manager, formerly ACE/Server]) as the tokens are purchased. On-demand tokens are also available, which provide a **tokencode** via email or SMS delivery, eliminating the need to provision a token to the user.

The token hardware is designed to be tamper-resistant to deter reverse engineering. When software implementations of the same algorithm (“software tokens”) appeared on the market, public code had been developed by the security community allowing a user to emulate **RSA SecurID** in software, but only if they have access to a current **RSA SecurID** code, and the original 64-bit **RSA SecurID** seed file introduced to the server. Later, the 128-bit **RSA SecurID** algorithm was published as part of an open source library. In the **RSA SecurID** authentication scheme, the seed record is the secret key used to generate one-time passwords. Newer versions also feature a USB connector, which allows the token to be used as a smart card-like device for securely storing certificates.

Source: https://en.wikipedia.org/wiki/RSA_SecurID

See also: RSA SecureID and Two-Factor Authentication (2FA)

From:
https://www.omgwiki.org/dido/ - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:r:rsa_secureid

Last update: **2022/02/17 08:57**