**It has been suggested that an independent certification authority should be established. Vendors would submit their components to this authority, which would validate that the component was trustworthy What would be the advantages and disadvantages of such a certification authority?**

Step 1:

A reputable organisation that issues Secure Sockets Layer (SSL) certificates is known as a certificate authority (CA). These digital certificates are data files that are used to link an entity cryptographically to a public key. They enable trust in online content delivery by allowing web browsers to validate material sent from web servers.

Comodo, GeoTrust, and Symantec are a few examples. Simply put, becoming a Certificate Authority (CA) involves taking control of the process of producing cryptographic pairs of private keys and public certificates.

Step 2:

The benefits of having a reliable third party guarantee that a component is reliable are obvious. Providing The quality of a system that indicates the level of user confidence that it will perform as intended is called trustworthiness. A trustworthy person must be accessible, dependable, safe, and secure.

Disadvantage: A certificate authority serves as a third-party issuer to guarantee the certificate's acceptance. In order to continue using the component, certification authorities often require a membership to their services. As a result, the cost of the component is a consideration.