


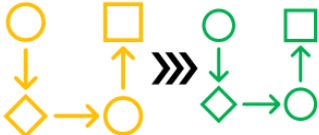
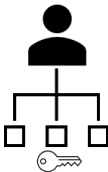
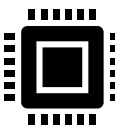
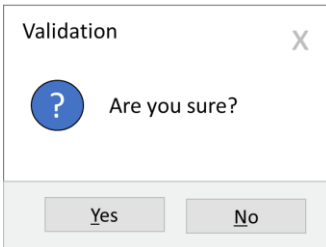
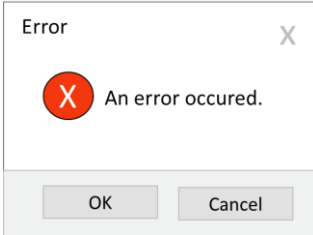



| Name | Description |
|--|---|
| Access Control Solution  | To determine whether or not a person has access to the system; several types of authentications. |
| Cryptographic authenticator  | Any form of authentication that uses encryption. |
| Connected keys with a push to authenticate  | A cryptographic device that enables two-factor authentication. For example, you must press the button to access your online bank. Without this pressure, you cannot authenticate. |
| Deserialization  | Serialization is the process of turning some object into a data format that can be restored later. People often serialize objects in order to save them to storage, or to send as part of communications. Deserialization is the reverse of that process, taking data structured from some format, and rebuilding it into an object. Today, the most popular data format for serializing data is JSON. Before that, it was XML. |
| Federated Login  | Enables users to use a single authentication ticket/token to obtain access across all the networks of the different IT systems. As a result, once the identity provider's authentication is complete, they now also have access to the other federated domains. The users don't have to perform any other separate login processes. |
| FIDO (Fido alliance is a company) | The FIDO Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. The FIDO Alliance promotes the development of, use of, and compliance with standards for authentication and device attestation. |
| Hardware security module  | A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions. |
| Intent to authenticate  | This verifies whether the user actually wants to access the system (checking if the person wants to authenticate), e.g., by displaying the message "are you sure you want to log in?". |
| Last Resort Error Handler  | We want to detect all errors - even those that we did not anticipate, so the system returns an error message. |
| Multi-factor authentication  | Authentication using at least three authentication factors, e.g., digital certificate + password + SMS |