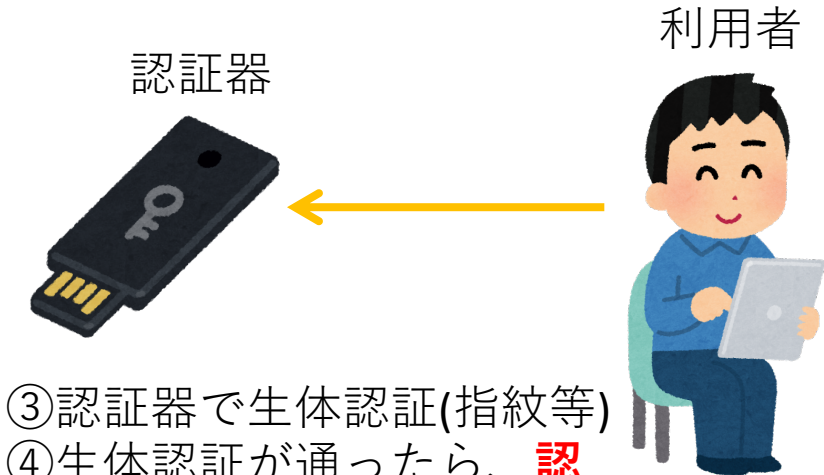
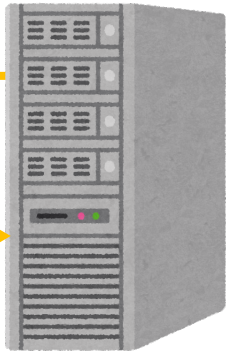
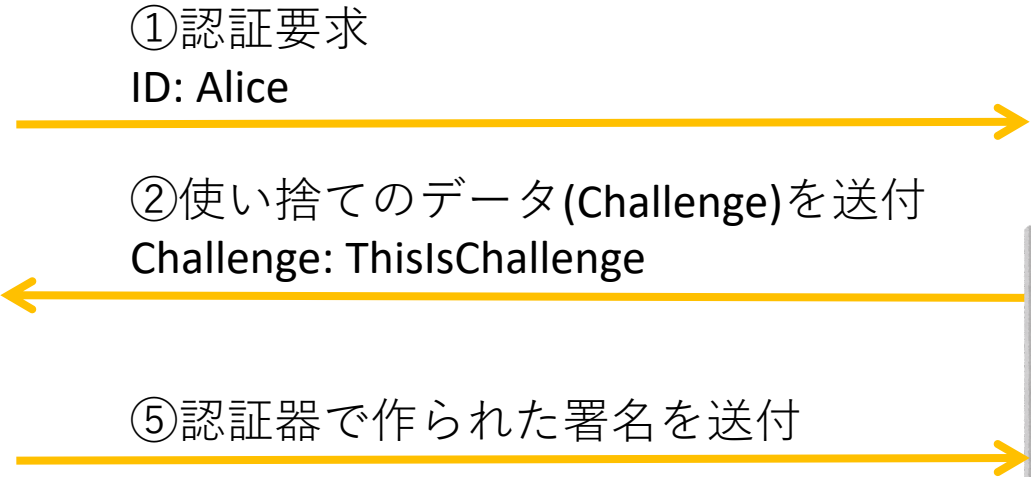


利用者の公開鍵を保存



- ③ 認証器で生体認証(指紋等)
- ④ 生体認証が通ったら、**認証器内部のみにある秘密鍵でチャレンジに対する署名を生成**

Signature: ThisIsSignature



- ⑥ あらかじめ保存していた公開鍵で、チャレンジに対する署名を検証

ID	公開鍵
Alice	0xXXXXXX....
Bob	0xYYYYYY....
Carol	0xZZZZZZ....