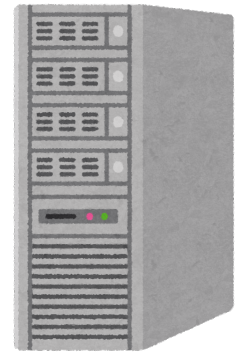
認証器

利用者

①認証要求
ID: Alice

利用者の公開鍵を保存



②使い捨てのデータ(Challenge)を送付
Challenge: ThisIsChallenge

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

⑤認証器で作られた署名を送付

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

検証が成功する正しい署名を作れるのは認証器を持つユーザ本人だけと考えられる！

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