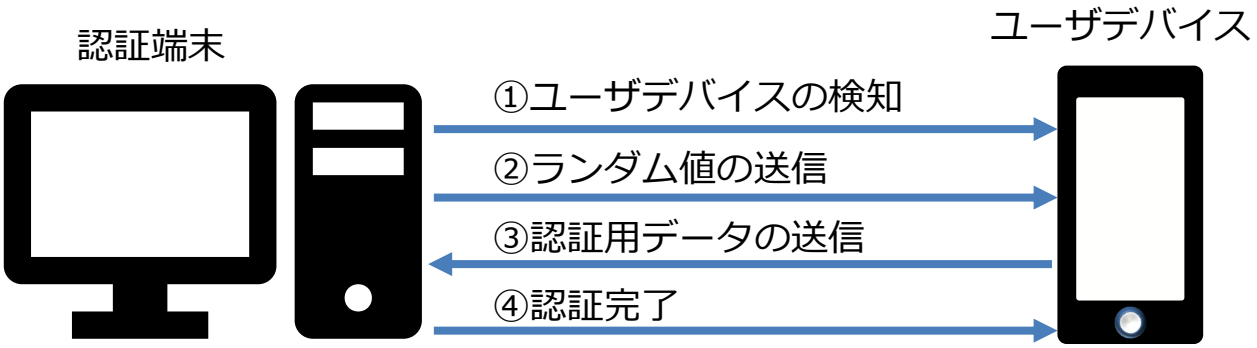
認証プロセスの概要

Bluetoothを用いた軽量コンパクトで、信頼性の高い本人認証を実現。



① 認証端末はユーザデバイスを検知する。

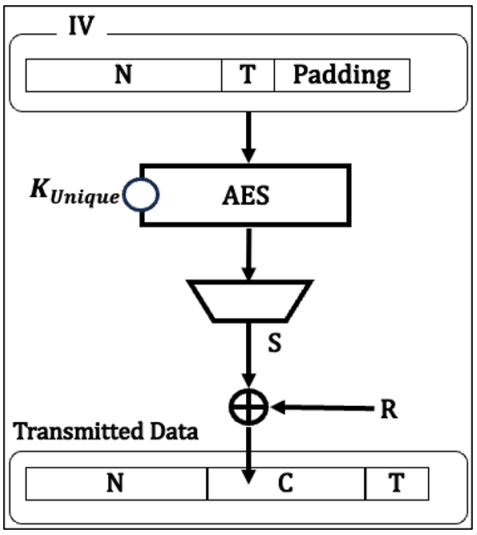
② 認証端末は検知したユーザデバイスにランダムな数値を設定。これをユーザデバイスに対して送信する。

③ ランダム値を受け取ったユーザデバイスは、これを暗号化。データの送信時刻やユーザIDと合わせて、認証端末に送信する。このとき、暗号化のIVに送信時刻とユーザIDを挿入することで改ざん検知を兼ねる。

④ 認証端末は受け取ったデータを複合化。返されたランダム値及び、送信時刻とデータを受け取った受信時刻を検証。異常がなければそのIDを認証完了とする。

認証用データの構成

暗号化の場合

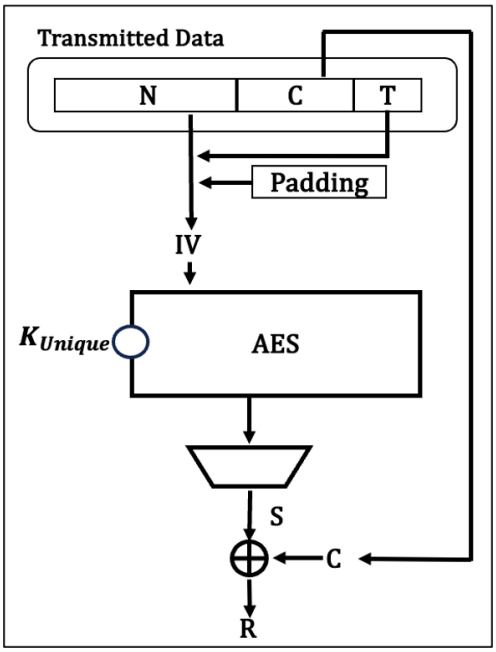


① N（ユーザID＋送信時刻）とT（その他付加情報）をもとにIV（initial vector）を生成し、鍵長32byteのユーザ別暗号鍵Kを用いてAES暗号化を行う。

② S（AES暗号化されたIV）とR（ランダム値）の排他的論理和を計算し、C（暗号化ランダム値）を得る。

③ N（ユーザID＋送信時刻）C（暗号化ランダム値）T（その他付加情報）を鍵長32byteのユーザ共通鍵でAES暗号化し認証端末へ送信する。

複合化の場合



① 受信したデータをユーザ共通鍵で複合化し、N（ユーザID＋送信時刻）C（暗号化ランダム値）T（その他付加情報）を得る。

② N（ユーザID＋送信時刻）T（その他付加情報）をもとにIVを生成。暗号化時と同様にしてSを生成する。

③ SとC（暗号化ランダム値）の排他的論理和を計算し、R（ランダム値）を得る。

④ このランダム値が認証端末側で割り振ったものと同じ値であれば、第三者による改ざんはないと判断する。

関連特許

その１・・・特許6751863

その２・・・特許6732326

その３・・・特願2024-005185