公募カテゴリーの事務局選出暗号2

エンティティ認証に関する事務局選出技術

CRYPTREC事務局

CRYPTREC
Cryptography Research and Evaluation Committees

事務局選出技術の選出基準

・国際標準技術など相互運用性上最低限必要な技術

・リストガイド作成時にWGによって安全性評価が確認されたもの

・リストガイド作成時にWGによって標準化動向が確認されたもの

CRYPTREC
Cryptography Research and Evaluation Committees

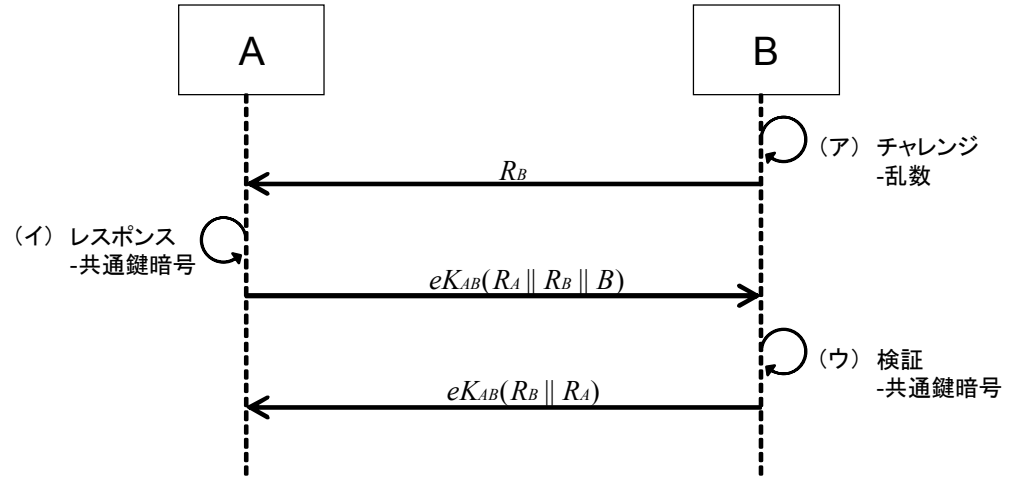
事務局選出技術カテゴリ

・128bitブロック暗号　なし

・エンティティ認証 3件(ISO/IEC 9798-2, ISO/IEC 9798-3, ISO/IEC 9798-4)

CRYPTREC
Cryptography Research and Evaluation Committees

エンティティ認証 1　ISO/IEC 9798-2



・共通鍵暗号を用いたエンティティ認証プロトコル

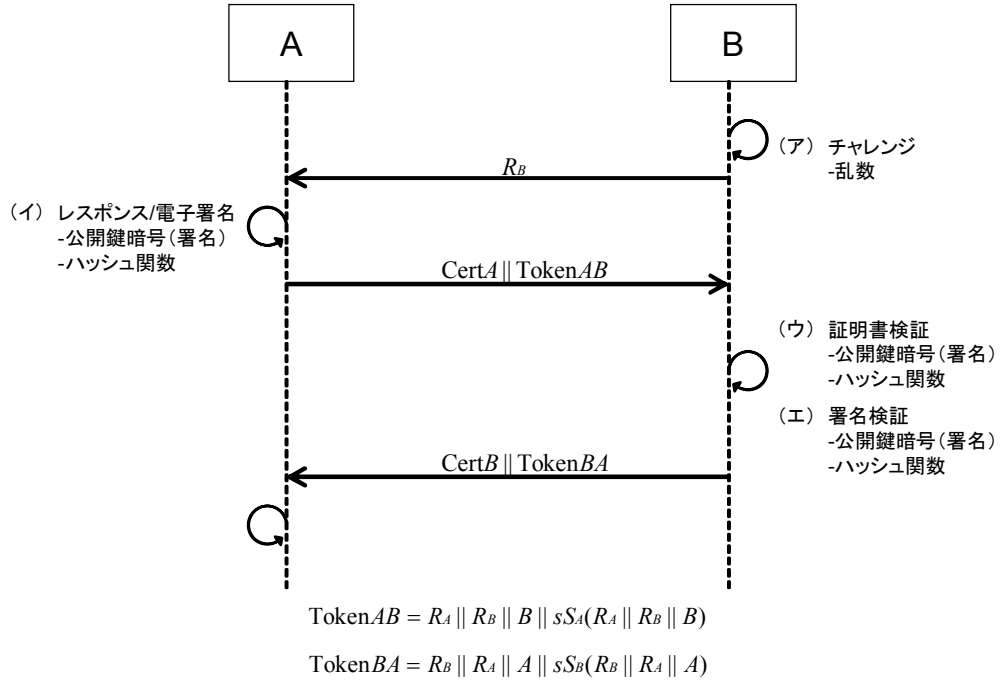
・認証を行うエンティティ同士が共通の秘密情報を有する

・チャレンジ-レスポンスプロトコルを利用して、認証を行う。そのため、疑似乱数生成をプロトコルに含む

・レスポンスは、共通鍵暗号アルゴリズムを用いたデータの暗号化で計算する

CRYPTREC
Cryptography Research and Evaluation Committees

エンティティ認証2 ISO/IEC 9798-3



・電子署名を用いたエンティティ認証プロトコル

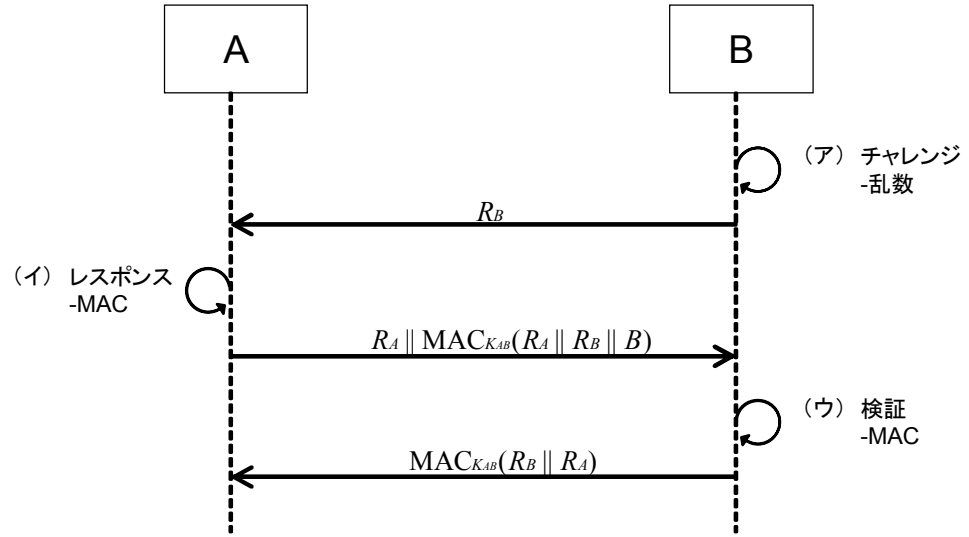
・認証を受ける側が自身の秘密鍵で処理を行い、対応する公開鍵を用いて認証結果を出力する

・チャレンジ-レスポンスプロトコルを利用した構成であるため、疑似乱数生成をプロトコルに含む

・PKIなどで、公開鍵の正しさが確保されていることが前提

CRYPTREC
Cryptography Research and Evaluation Committees

エンティティ認証3 ISO/IEC 9798-4



・検査関数（メッセージ認証子）を用いたエンティティ認証プロトコル

・認証を行うエンティティ同士が共通の秘密情報を有する

・チャレンジ-レスポンスプロトコルを利用して、認証を行う。そのため、疑似乱数生成をプロトコルに含む。

・レスポンスは、MACアルゴリズムを用いて計算する

CRYPTREC
Cryptography Research and Evaluation Committees