暗号プロトコル評価対象の概要

独立行政法人　情報通信研究機構

1.プロトコル名：Basic Access Control (ISO/IEC 11770-2-6)

2.関連する標準：Machine Readable Travel Documents Technical Report

http://www.csca-si.gov.si/TR-PKI_mrtds_ICC_read-only_access_v1_1.pdf

3.暗号プロトコル仕様

Basic Access Control (e-Passport) について解説する。

3.1.暗号プロトコルの概要と目的

IC旅券に内蔵されたチップ(MRTD)と、検査システム(IFD)のBIS端末(カードリーダ)との間で相互認証を行い、セッション鍵を共有するため暗号プロトコル。セッション確立後に、IC旅券に記録されている個人データ通信が開始される。

シーケンス図

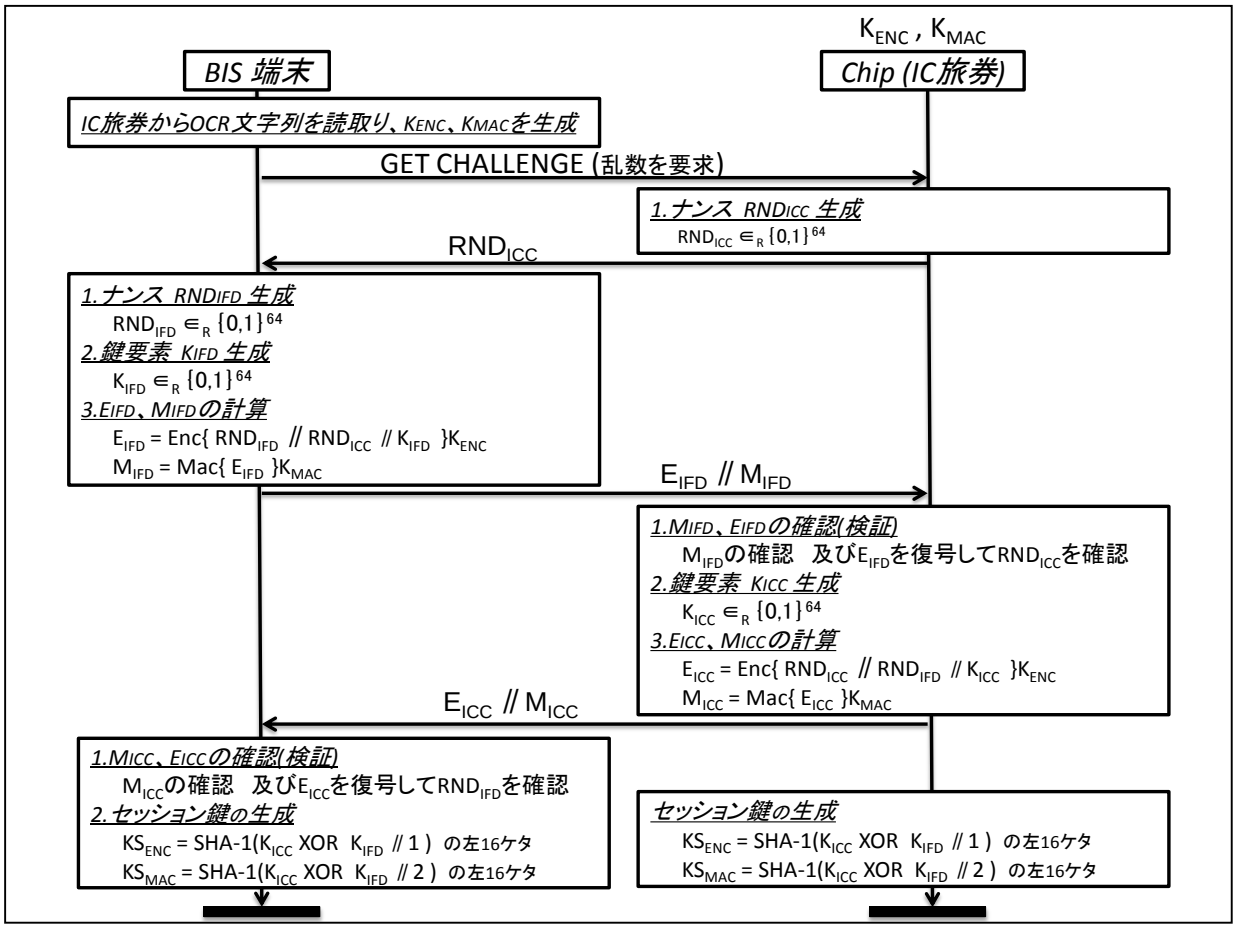

図 1. シーケンス図

（※１）：IC 旅券から読み取った MRZ(Machine Readable Zone)情報として、「旅券番号」「生年月日」「有効期限」「チェックデジット」を SHA-1 に入力し、K_{SEED} を作成する。その後、K_{SEED} を元に再度 SHA-1 を用いて K_{ENC} 及び K_{MAC} を生成する。

4. 評価の環境

4.1. 攻撃者モデル（自然言語による記述）

エラー！参照元が見つかりません。の文献では、特に攻撃者モデルに関する記述はないが、数メートル離れた地点から通信の盗聴が可能であることを指摘している。無線通信では、通信の盗聴及び不正パケットの送信が容易である一方、通信パケットを差し替えることは困難である。しかし、ここでは評価を単純化するため、より強い攻撃者を仮定する Dolev-Yao モデルに沿って評価を行う。ただし、事前共有鍵 Kseed を生成するために用いられる MRZ_info については、安全な通信路で共有されるものと仮定する。この値は、パスポート

に記載された情報から算出可能であるため、パスポートの一時的な盗難により、BAC プロトコルは脆弱な状況に陥ることに留意すべきである。

4.2.セキュリティプロパティ（自然言語による記述）

相互認証プロトコルでは、2 つのロールが互いの存在を確認し、通信相手が嘘をついていないと確認することが目的である。

・ロール P がロール A を認証すること。

・ロール A がロール P を認証すること。

また、セッション鍵は暗号プロトコルを通じて共有された秘密情報 Ka, Kp から KDF (Key Derivation Function)を用いて生成されるため、セッション鍵の秘匿性は、Ka と Kp の秘匿性に帰着される (Ka と Kp のいずれかが秘匿性を有していればよい)。

・Ka が秘匿性を満たすこと。

・Kp が秘匿性を満たすこと。

4.3.暗号プロトコルに関して知られている結果

MRTD の Basic Access Control については、下記の結果が知られている。

(a) Vijayakrishnan Pasupathinathan and Josef Pieprzyk , Huaxiong Wang . Security Analysis of Australian and E.U. E-passport Implementation .Journal of Research and Practice in Information Technology , vol.40 , No.3 , August 2008.
http://www.jrpit.acs.org.au/jrpit/JRPITVolumes/JRPIT40/JRPIT40.3.187.pdf

(b) Vijayakrishnan P , Josef Pieprzyk , Huaxiong Wang , Formal Security Analysis of Australian E-passport Implementation .
http://crpit.com/confpapers/CRPITV81Vijayakrishnan.pdf

(c) Vijayakrishnan Pasupathinathan, Josef Pieprzyk, and Huaxiong Wang . An On-Line Secure E-Passport Protocol. IPSEC 2008 , LNCS 4991 ,pp.14-28,2008.
http://www.vkrishnan.com/Research/publications_assets/2008ISPEC.pdf

5.備考

本文書は、**総務省「暗号・認証技術等を用いた安全な通信環境推進事業に関する実証実験の請負　成果報告書**」からの引用である。