ISO/IEC 9798 プロトコルの安全性評価

山村明弘
秋田大学大学院工学資源学研究科

2011 年 2 月 4 日

概 要

ISO/IEC 9798-2 (Mechanisms using symmetric encipherment algorithms), ISO/IEC 9798-3 (Mechanisms using digital signature techniques), ISO/IEC 9798-4 (Mechanisms using a cryptographic check function) におけるエンティティ認証技術の安全性評価を行なう。

1 はじめに

本評価報告書で、ISO/IEC で国際標準技術となっている認証メカニズム（9798-2, 9798-3, 9798-4）に関する安全性評価について述べる。ISO/IEC で国際標準技術となっている認証メカニズム（9798-2, 9798-3, 9798-4）の技術仕様、考えられる攻撃手法、安全性について議論する。形式的手法については，今回考慮せずに、安全性について検討を行っている。

2 応募暗号への要請と評価事項

電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）において、エンティティ認証に関する応募技術には、以下が要請されている。

電子政府推奨暗号リストに掲載された共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証、あるいは、安全性を計算量的な困難さに帰着できるエンティティ認証を公募します。エンティティ認証を構成する要素技術は、現リストに掲載されている暗号技術を用いることを原則とします。要素技術として、現リストに掲載されていない共通鍵暗号、メッセージ認証コードを用いる場合は、これらの要素技術を同時に応募する必要があります。また、上記以外の要素技術を用いたエンティティ認証技術の応募も可能です。

また評価項目に関しては、以下のように安全性評価と実装性能評価が求められている。

（1）安全性評価項目
安全性の評価は、エンティティ認証としてのセキュリティに問題が生じないことを、形式的な手法を用いて行います。安全性を脅かす状態としては、なりすましの成功、セッションの取り換え等を想定します。暗号プリミティブとして、電子政府推奨暗号リストに掲載されている、あるいは応募中の共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードのみを利用している場合には、暗号プリミティブを理想的に安全なものとして安全性の評価を行います。その他の暗号プリミティブを用いる場合には、暗号プリミティブを理想化せずに安全性の検証を行います。上記のいずれの場合も、提案者はプロトコルの安全性を示す情報を提出し、本公募における安全性評価では、これらの正当性を検証します。

（2）実装性評価項目
エンティティ認証プロトコルの実装性能評価として、ソフトウェアによる実装性評価を行います。標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。通信時間は考慮しません。

3 エンティティ認証の機能、安全性評価の仮定

3.1 実現する機能

エンティティ認証プロトコルが実現するべき機能として片側認証、両側認証、鍵共有、forward security などがある。今回の安全性評価においても、電子政府構成に必要とされるこれらの機能の実現可能性について解析する。評価対称となる認証プロトコルが達成する機能を表に示す。

3.2 仮定

暗号プリミティブとして、電子政府推奨暗号リストに掲載されている、あるいは応募中の共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードのみを利用している場合には、暗号プリミティブを理想的に安全なものと仮定する。IOTP の技術仕様書から利用可能と示唆される電子政府推奨暗号に属する公開鍵暗号技術には、DSA, ECDSA, RSASSA-PKCS1-v1_5, RSA-PSS, RSA-OAEP, RSAES-PKCS1-v1_5 [15, 16, 14] がある。これらの技術を IOTP の実装との整合性について考察する。

3.3 Abadi, Needham によるプロトコル設計における注意点

M.Abadi と R.Needham が [1] において暗号プロトコル設計において注意するべき 11 点の事柄を原則としてまとめている。暗号プロトコル設計指針の基本となるべきものであるので、ここで確認を行い、評価対象にそれぞれにおいて確認する。少なくとも、Abadi と Needham

によるプロトコル設計における原則が守られているかどうか検証し、原則が守られていない場合には、それに起因する安全性の問題点を指摘する。

1. プロトコルにおいて送受信されるすべてのメッセージは、それが何のためのものか明確にしなければならない
2. メッセージに対して対応するべきかどうか決定する条件を明確に定める
3. メッセージにおいて、認証者、被認証者のアイデンティティが重要である場合は、メッセージに名前を明示する
4. 暗号化処理が施される場合には、その目的を明確にする
5. 暗号文に署名する場合には、暗号文に対応する平文を知っていると推論されてはいけない。一方で、署名を行い、その後暗号化する場合には、平文を知っていると推論される
6. Nonce (Number used once) が満たすべき性質が何か明確にせよ
7. （カウンターなどの）予知可能な数は、チャレンジーリスポンスにおいてフレッシュであることに役立つが、攻撃者がチャレンジをシミュレートしてリスポンスをリプレイする事を避けられるように守られていなければならない。
8. タイムスタンプが利用される場合には、種々のマシンの時刻同期は許容範囲におさめる
9. 鍵が nonce の暗号化等に最近利用された事は、けっして、その鍵が安全であるとは意味しない
10. メッセージが符号化される時は、どの符号化が使われているか分からなければならない。メッセージが実行しているプロトコルに属し、そのプロトコルの何番目のメッセージにあたるのか分かることが可能でなければならない。
11. プロトコル設計者はどのトラスト関係に依存するのか知っているべきである。

後述するように、無限ワンタイムパスワード認証方式（IOTP）においては、原則 1, 2, 3, 4, 10, 11 が守られていない。

4 ISO/IEC（9798-2, 9798-3, 9798-4）の技術仕様

4.1 技術仕様

ISO/IEC（9798-2, 9798-3, 9798-4）において、Time variant parameter は以前通信されたデータが再び送信された場合にそれを検知する事に利用される。ISO/IEC（9798-2, 9798-3, 9798-4）では、Time variant parameter として、タイムスタンプ、シーケンス番号、乱数を利

用する。乱数の生成については。ISO/IEC 18031 に従うものとされている。以下で、ISO/IEC（9798-2, 9798-3, 9798-4）の各方式の通信フローを図示する。

A, B はエンティティを表す。e_K は秘密鍵 K による暗号化関数を表す。I_U は I のアイデンティティを表す。K_{UV} はエンティティU と V により共有されている秘密鍵を表す。N_U は U により発行されたシーケンス番号を表す。P は信頼される第三者機関を表す。R_U は U により生成された乱数を表す。TN_U は U により発行された Time variant parameter を表し、タイムスタンプまたはシーケンス番号を表す。$Token_{UV}$ は U から V に送信されるトークンを表す。T_U は U により発行されたタイムスタンプを表す。TVP_U は U により発行された Time variant parameter を表し、タイムスタンプ、シーケンス番号、または乱数を表す。$X||Y$ は X と Y の連結を表す。$sS(Y_1||\cdots||Y_j)$ は $Y_1||\cdots||Y_j$ を入力として生成された署名を表す。$f_K(X)$ は K を鍵として暗号チェック関数 f 作用させた値を表す。

4.2 ISO/IEC 9798-2

ISO/IEC 9798-2 は共通鍵暗号技術を利用したエンティティ認証技術であり、片側認証と両側認証、信頼できる第三者機関の仮定の有無、通信の回数により 6 つに分類される。また、それぞれの方式において、Time variant parameter として、タイムスタンプ、シーケンス番号、乱数を利用する。

この認証方式においては、秘密情報である認証鍵を所有している事を証明することによって認証が実現される。乱数の扱いについては ISO/IEC 18031 に従うものとされる。タイムスタンプには、Coordinate Universal Clock (UTC) が推奨されている（ISO/IEC 9798-1）。ISO/IEC 9798-2 においては、あるデータを秘密の鍵で暗号化することで、その鍵の所有を証明する仕組みである。そのデータには、Time variant parameter が含まれていないといけない。Time variant parameter が乱数である場合には、送信したデータと同一である事を確認することが必要である。Time variant parameter がタイムスタンプである場合には、タイムスタンプの妥当性を確認しなければならない。Time variant parameter がシーケンス番号である場合には、保持しているシーケンス番号と比べて、リプレイでないことを確認しなければならない。

4.2.1 Mechanism 1-One-pass authentication

Mechanism 1-One-pass authentication は片側認証を実現する技術である。

$$1.\ A \Longrightarrow B : Token_{AB}$$
$$Token_{AB} = Text_2||e_{K_{AB}}(TN_A||I_B||Text_1)$$

図 1: Mechanism 1-One-pass authentication

4.2.2 Mechanism 2-Two-pass authentication

Mechanism 2-Two-pass authentication は片側認証を実現する技術である。

$$
\begin{gathered}
1.\ B \Longrightarrow A : R_B||Text_1 \\
2.\ A \Longrightarrow B : Token_{AB} \\
Token_{AB} = Text_3||e_{K_{AB}}(R_B||I_B||Text_2)
\end{gathered}
$$

図 2: Mechanism 2-Two-pass authentication

4.2.3 Mechanism 3-Two-pass authentication

Mechanism 3-Two-pass authentication は両側認証を実現する技術である。

$$
\begin{gathered}
1.\ A \Longrightarrow B : Token_{AB} \\
2.\ B \Longrightarrow A : Token_{BA} \\
Token_{AB} = Text_2||e_{K_{AB}}(TN_A||I_B||Text_1) \\
Token_{BA} = Text_4||e_{K_{AB}}(TN_B||I_B||Text_3)
\end{gathered}
$$

図 3: Mechanism 3-Two-pass authentication

4.2.4 Mechanism 4-Three-pass authentication

Mechanism 4-Three-pass authentication は両側認証を実現する技術である。

$$
\begin{gathered}
1.\ B \Longrightarrow A : R_B||Text_1 \\
2.\ A \Longrightarrow B : Token_{AB} \\
3.\ B \Longrightarrow A : Token_{BA} \\
Token_{AB} = Text_3||e_{K_{AB}}(R_A||R_B||I_B||Text_2) \\
Token_{BA} = Text_5||e_{K_{AB}}(R_B||R_A||Text_4)
\end{gathered}
$$

図 4: Mechanism 4-Three-pass authentication

4.2.5 Mechanism 5-Four-pass authentication

Mechanism 5-Four-pass authentication は両側認証を実現する技術である。信頼された第三者機関を仮定する。

$$
\begin{gathered}
1.\ A \Longrightarrow P : TVP_A||I_B||Text_1 \\
2.\ P \Longrightarrow A : Token_{PA} \\
3.\ A \Longrightarrow B : Token_{AB} \\
4.\ B \Longrightarrow A : Token_{BA} \\
Token_{PA} = Text_4||e_{K_{AP}}(TVP_A||K_{AB}||I_B||Text_3)||e_{K_{BP}}(TN_P||K_{AB}||I_A||Text_2) \\
Token_{AB} = Text_6||e_{K_{BP}}(TN_P||K_{AB}||I_A||Text_2)||e_{K_{BP}}(TN_A||I_B||Text_5) \\
Token_{BA} = Text_8||e_{K_{AB}}(TN_B||I_A||Text_7)
\end{gathered}
$$

図 5: Mechanism 5-Four-pass authentication

4.2.6 Mechanism 6-Five-pass authentication

Mechanism 6-Five-pass authentication は両側認証を実現する技術である。信頼された第三者機関を仮定する。

$$
\begin{gathered}
1.\ B \Longrightarrow A : R_B||Text_1 \\
2.\ A \Longrightarrow P : R_A||R_B||I_B||Text_2 \\
3.\ P \Longrightarrow A : Token_{PA} \\
4.\ A \Longrightarrow B : Token_{AB} \\
5.\ B \Longrightarrow A : Token_{BA} \\
6.\ Token_{PA} = Text_5||e_{K_{AP}}(R_A||K_{AB}||I_B||Text_4)||e_{K_{BP}}(R_B||K_{AB}||I_A||Text_3) \\
Token_{AB} = Text_7||e_{K_{BP}}(R_B||K_{AB}||I_A||Text_3)||e_{K_{AB}}(R'_A||R_B||Text_6) \\
Token_{BA} = Text_9||e_{K_{AB}}(R_B||R'_A||Text_8)
\end{gathered}
$$

図 6: Mechanism 6-Five-pass authentication

4.3 ISO/IEC 9798-3

ISO/IEC 9798-3 は電子署名技術を利用したエンティティ認証技術であり、片側認証と両側認証、信頼できる第三者機関の仮定の有無、通信の回数により 7 つに分類される。また、そ

れぞれの方式において、Time variant parameter として、タイムスタンプ、シーケンス番号、乱数を利用する。この認証方式においては、秘密情報である認証鍵を所有している事を証明することによって認証が実現される。乱数の扱いについては ISO/IEC 18031 に従うものとされる。タイムスタンプには、Coordinate Universal Clock (UTC) が推奨されている（ISO/IEC 9798-1）。ISO/IEC 9798-2 においては、あるデータを秘密の鍵で暗号化することで、その鍵の所有を証明する仕組みである。そのデータには、Time variant parameter が含まれていないといけない。Time variant parameter が乱数である場合には、送信したデータと同一である事を確認することが必要である。Time variant parameter がタイムスタンプである場合には、タイムスタンプの妥当性を確認しなければならない。Time variant parameter がシーケンス番号である場合には、保持しているシーケンス番号と比べて、リプレイでないことを確認しなければならない。

4.3.1 Mechanism 1-One-pass authentication

Mechanism 1-One-pass authentication は片側認証を実現する技術である。

$$\begin{gathered} 1.\ A \Longrightarrow B : Cert_A || Token_{AB} \\ Token_{AB} = \begin{matrix} T_A \\ N_A \end{matrix} ||B||Text2||sS_A(\begin{matrix} T_A \\ N_A \end{matrix} ||B||Text1) \end{gathered}$$

図 7: Mechanism 1-One-pass authentication

4.3.2 Mechanism 2-Two-pass authentication

Mechanism 2-Two-pass authentication は片側認証を実現する技術である。

$$\begin{gathered} 1.\ B \Longrightarrow A : R_B||Text1 \\ 2.\ A \Longrightarrow B : Cert_A||Token_{AB} \\ Token_{AB} = R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2) \end{gathered}$$

図 8: Mechanism 2-Two-pass authentication

4.3.3 Mechanism 3-Two-pass authentication

Mechanism 3-Two-pass authentication は両側認証を実現する技術である。

$$
\begin{array}{c}
1.\ A \Longrightarrow B : Cert_A || Token_{AB} \\
2.\ B \Longrightarrow A : Cert_B || Token_{BA} \\
Token_{AB} = \begin{matrix} T_A \\ N_A \end{matrix} ||B||Text2||sS_A(\begin{matrix} T_A \\ N_A \end{matrix} ||B||Text1) \\
Token_{BA} = \begin{matrix} T_B \\ N_B \end{matrix} ||A||Text4||sS_B(\begin{matrix} T_B \\ N_B \end{matrix} ||A||Text3)
\end{array}
$$

図 9: Mechanism 3-Two-pass authentication

4.3.4 Mechanism 4-Three-pass authentication

Mechanism 4-Three-pass authentication は両側認証を実現する技術である。

$$
\begin{array}{c}
1.\ B \Longrightarrow A : R_B || Text1 \\
2.\ A \Longrightarrow B : Cert_A || Token_{AB} \\
3.\ B \Longrightarrow A : Cert_B || Token_{BA} \\
Token_{AB} = R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2) \\
Token_{BA} = R_B||R_A||A||Text5||sS_B(R_B||R_A||A||Text4)
\end{array}
$$

図 10: Mechanism 4-Three-pass authentication

4.3.5 Mechanism 5-Two-pass parallel authentication

Mechanism 5-Two-pass parallel authentication は両側認証を実現する技術である。

$$
\begin{array}{c}
1.\ A \Longrightarrow B : Cert_A || R_A || Text1 \\
1'.\ B \Longrightarrow A : Cert_B || R_B || Text2 \\
2.\ B \Longrightarrow A : Token_{BA} \\
2'.\ A \Longrightarrow B : Token_{AB} \\
Token_{AB} = R_A||R_B||B||Text4||sS_A(R_A||R_B||B||Text3) \\
Token_{BA} = R_B||R_A||A||Text6||sS_B(R_B||R_A||A||Text5)
\end{array}
$$

図 11: Mechanism 5-Two-pass parallel authentication

4.3.6 Five pass authentication (initiated by A)

Five pass authentication (initiated by A) は両側認証を実現する技術である。

1. $A \Longrightarrow B : R_A||I_A||Text_1$
2. $B \Longrightarrow A : I_B||Token_{BA}$
3. $A \Longrightarrow P : R'_A||R_B||I_A||I_B||Text4$
4. $P \Longrightarrow A : Text7||TokenTA$
5. $A \Longrightarrow B : Token_{AB}$

Option 1

$$Token_{AB} = Text_9||ResA||sS_T(R_B||ResA||Text5)||sS_A(R_B||R_A||B||A||Text8)$$
$$Token_{BA} = R_A||R_B||Text3||sS_B(B||R_A||R_B||A||Text2)$$
$$Token_{TA} = ResA||ResB||sS_T(R'_A||ResB||Text6)||sS_T(R_B||ResA||Text5)$$

Option 2

$$Token_{AB} = R'_A||Text_9||TokenTA||sS_A(R_B||R_A||B||A||Text8)$$
$$Token_{BA} = R_A||R_B||Text3||sS_B(B||R_A||R_B||A||Text2)$$
$$Token_{TA} = ResA||ResB||sS_T(R'_A||R_B||ResA||ResB||Text5)$$

$I_A = A$ or $CertA$
$I_B = B$ or $CertB$
$ResA = (CertA||Status), (A||P_A)$ or $Failure$
$ResB = (CertB||Status), (B||P_B)$ or $Failure$

図 12: Five pass authentication (initiated by A)

4.3.7 Five pass authentication (initiated by B)

Five pass authentication (initiated by B) は両側認証を実現する技術である。

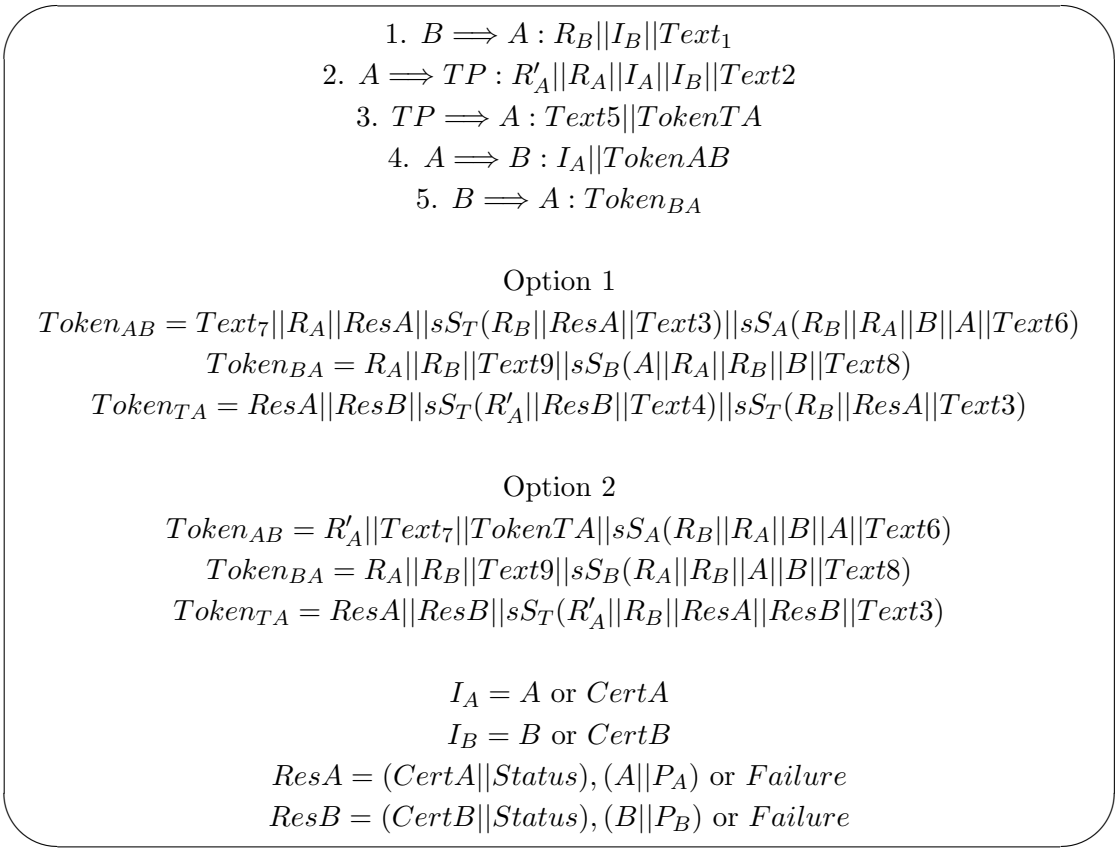

図 13: Five pass authentication (initiated by B)

4.4 ISO/IEC 9798-4

ISO/IEC 9798-4 は暗号チェック関数（CCF）を利用したエンティティ認証技術であり、片側認証と両側認証、通信の回数により 4 つに分類される。また、それぞれの方式において、Time variant parameter として、タイムスタンプ、シーケンス番号、乱数を利用する。この認証方式においては、秘密情報である認証鍵を所有している事を証明することによって認証が実現される。乱数の扱いについては ISO/IEC 18031 に従うものとされる。タイムスタンプには、Coordinate Universal Clock (UTC) が推奨されている（ISO/IEC 9798-1）。

ISO/IEC 9798-4 においては、あるデータを秘密の鍵を用いて暗号チェック関数値を計算することで、その鍵の所有を証明する仕組みである。そのデータには、Time variant parameter が含まれていないといけない。Time variant parameter が乱数である場合には、送信したデータと同一である事を確認することが必要である。Time variant parameter がタイムスタンプである場合には、タイムスタンプの妥当性を確認しなければならない。Time variant parameter

がシーケンス番号である場合には、保持しているシーケンス番号と比べて、リプレイでないことを確認しなければならない。

4.4.1 Mechanism 1-One-pass authentication

Mechanism 1-One-pass parallel authentication は片側認証を実現する技術である。

$$1.\ A \Longrightarrow B : Token_{AB}$$
$$Token_{AB} = \begin{matrix} T_A \\ N_A \end{matrix} ||Text2||f_{K_{AB}}(\begin{matrix} T_A \\ N_A \end{matrix} ||B||Text1)$$

図 14: Mechanism 1-One-pass authentication

4.4.2 Mechanism 2-Two-pass authentication

Mechanism 2-Two-pass parallel authentication は片側認証を実現する技術である。

$$1.\ B \Longrightarrow A : R_B||Text1$$
$$2.\ A \Longrightarrow B : Token_{AB}$$
$$Token_{AB} = Text3||f_{K_{AB}}(R_B||B||Text2)$$

図 15: Mechanism 2-Two-pass authentication

4.4.3 Mechanism 3-Two-pass authentication

Mechanism 3-Two-pass parallel authentication は両側認証を実現する技術である。

$$
\begin{array}{c}
1.\ A \Longrightarrow B : Token_{AB} \\
2.\ B \Longrightarrow A : Token_{BA} \\
Token_{AB} = \begin{matrix} T_A \\ N_A \end{matrix} ||Text2||f_{K_{AB}}(\begin{matrix} T_A \\ N_A \end{matrix} ||B||Text1) \\
Token_{BA} = \begin{matrix} T_B \\ N_B \end{matrix} ||Text4||f_{K_{AB}}(\begin{matrix} T_B \\ N_B \end{matrix} ||A||Text3)
\end{array}
$$

図 16: Mechanism 3-Two-pass authentication

4.4.4 Mechanism 4-Three-pass authentication

Mechanism 4-Three-pass authentication は両側認証を実現する技術である。

$$
\begin{array}{c}
1.\ B \Longrightarrow A : R_B||Text1 \\
2.\ A \Longrightarrow B : Token_{AB} \\
3.\ B \Longrightarrow A : Token_{BA} \\
Token_{AB} = R_A||Text3||f_{K_{AB}}(R_A||R_B||B||Text2) \\
Token_{BA} = Text5||f_{K_{AB}}(R_B||R_A||Text4)
\end{array}
$$

図 17: Mechanism 4-Three-pass authentication

5 ISO/IEC（9798-2, 9798-3, 9798-4）の安全性評価

ISO/IEC（9798-2, 9798-3, 9798-4）の各技術について、種々攻撃を考察してみたが、大きな問題は発見されなかった。しかし、9798-3 Three-pass mutual authentication は過去において、脆弱性を含んでおり改訂を行なった経緯がある。これは、[4] による攻撃が、過去の 9798-3 Three-pass mutual authentication に適用できたことによる。改訂された版と、過去の脆弱性を持つ版の差異は小さく、他の 9798 プロトコルに安全性に問題がないとは言い切れない。

1. ISO/IEC（9798-2, 9798-3, 9798-4）に属する多くの方式がある。その利用方法、使い分けについて ISO/IEC は指針を与えていない。電子政府における応用システムによって、適切な方式を選択する必要がある。

2. 一部の方式は複雑すぎて、安全性評価が難しい。認証プロトコルの安全性評価は極めて難しいためなるべく簡単な方式の方が安全性評価を実施しやすい。適切な暗号関数の選

択、適切な実装が前提とされるが、実システムの実装において脆弱性を含む原因となりやすい。

3. ISO/IEC（9798-2, 9798-3, 9798-4）では、Time variant parameter として、タイムスタンプ、シーケンス番号、乱数を利用する。各々、一長一短ある。タイムスタンプを利用する場合には時刻同期が前提となる。逆に、正確な時刻同期が実現されていない場合は、攻撃を許す結果になりやすい。一方、シーケンス番号を利用する場合には、同期を保ったままシーケンス番号を管理する。つまり、ステイトフルな状況を保持することになる。通信エラーなどによる同期のずれを修正する手法を用意する必要もある。また、通信者が少数である場合には、シーケンス番号を利用することにメリットがあるが、電子政府等の大規模なシステムの場合には、通信者毎にシーケンス番号を保持する事は現実的ではないと考えられる。電子政府側のサーバーが国民全体と通信する可能性があり、国民一人一人とシーケンス番号を同期させる事は現実的ではない。

ISO/IEC（9798-2, 9798-3, 9798-4）については、今後も継続的に安全性評価を行う必要があると考えられる。

参考文献

[1] M.Abadi and R.Needham, Prudent engineering practice for cryptographic protocols, DEC SRC Technical Report 125, Digital Equipment Corporation (1995)

[2] R.Anderson, Security Engineering : A Guide to Buiding Dependable Distributed Systems, John & Wiley Sons (2001)

[3] M.Burrows, M.Abadi, and R.Needham, A logic for authentication, SRC Technical Report 39, Digital Equipment Corporation (1989)

[4] W.Diffie, P.C.van Oorschot and M.Wiener, Authentication and authenticated key exchanges, Designs, Codes and Cryptography, 2 (1992) 107-125

[5] ISO/IEC Information Technology - Security Technology - Entity Authentication Part 1: General, ISO/IEC JTC 1/SC 27 DIS 9798-1: (1996)

[6] ISO/IEC Information Technology - Security Technology - Entity Authentication Part 2: Entity authentication using symmetric techniques, ISO/IEC JTC 1/SC 27 N489 CD 9798-2: (1992)

[7] ISO/IEC Information Technology - Security Technology - Entity Authentication Part 2: Entity authentication using symmetric techniques, ISO/IEC JTC 1/SC 27 N739 DIS 9798-2: (1993)

[8] ISO/IEC Information Technology - Security Technology - Entity Authentication Part 2: Mechanisms using symmetric encipherment algorithms, ISO/IEC JTC 1/SC 27 N2145 FDIS 9798-2: (1998)

[9] ISO/IEC Information Technology - Security Technology - Entity Authentication Part 3: Mechanisms using digital signature techniques, BS ISO/IEC 9798-3: (1998)

[10] ISO/IEC Information Technology - Security Technology - Entity Authentication Part 4: Mechanisms using a cryptographic check function, ISO/IEC JTC 1/SC 27 N2289 FDIS 9798-4: (1999)

[11] J.Katz and Y.Lindell, Introduction to Modern Cryptography, Chapman & Hall (2008)

[12] W.Mao, Modern Cryptography, Prentice Hall (2004)

[13] A.J.Menezes, P.C.van Oorschot and S.A.Vanstone, Handbook of Applied Cryptography, CRC Press (1997)

[14] DSA NIST FIPS 186-2 (+Change Notice 1)

[15] RSA PKCS #1 v2.1: RSA Cryptography Standard

[16] ECDSA SEC 1: Elliptic Curve Cryptography(September 20, 2000 Version 1.0)