**関係各部署 御中**

**To departments concerned**

| Confidential level | PROTECTED 関係者外秘 | 原紙保管 Storage of original | M/Y / |
|---|---|---|---|
| | | コピー保管 Storage of copy | M/Y / |

# 無線通信セキュリティ要求仕様書
# Requirements Specification of Wireless Communication Security


制御電子プラットフォーム開発部
制御ネットワーク・アーキ開発室 4G
E/E Architecture Development Div.
System network & architecture development dept. 4G


No. SEC-ePF-WLS-REQ-SPEC-a00-08-a

| 承認 Approved | 調査 Checked | 作成 Created | 2022/06/09 |
|---|---|---|---|
| 河井 | 松井 | 玉樹 | Omission of signature (approved electronically) |

| | |
|---|---|
| **適用 Scope** | 車載ネットワークに接続され、車外と無線通信を行う ECU に適用する。<br>Apply to ECUs which are connected to the in-vehicle network and communicate wirelessly with outside target of the vehicle. |
| **変更内容 Revision Record** | 【主な変更点 Main changes】<br>(SEC-ePF-WLS-REQ-SPEC-a00-07-a ⇒ SEC-ePF-WLS-REQ-SPEC-a00-08-a<br>・要件変更（Change requirements） |
| **特記 Special note** | 【展開ルール Distribution rule】<br>必要に応じて、関係会社・関係部署（海外事業体、ボデーメーカ、ECU サプライヤ）への展開をお願いします。<br>Please distribute this document to affiliated companies, or departments (e.g. overseas business entities, car body manufacturers, or ECU suppliers) if necessary.<br><br>【問合せ先 Contact Information】<br>制御電子プラットフォーム開発部 制御ネットワーク・アーキ開発室<br>セキュリティ仕様問合せ窓口<br>E/E Architecture Development Div. System network & architecture development dept.<br>Contact for security inquiries<br>E-mail: epf-sec-sp@mega.tec.toyota.co.jp |

# 1. 変更履歴

| Version | 変更内容 | 日付 | 変更者 |
|---|---|---|---|
| a00-00-a | 新規作成 | 2021/04/01 | 46F 垣屋 |
| a00-00-b | 英訳を追加 | 2021/05/31 | 46F 清川 |
| | セキュリティ関連用語は SEC-ePF-TRM-GUD-PROC-***-**-*に記載されているため、2.5 用語を削除 | | |
| | 要件 ID の誤記修正(番号は変更なし)<br>WSECR_***** ⇒ WLSREQ_***** | | |
| | 上位文書の明確化 | | |
| | Appendix A の追加 | | |
| a00-01-a | 3.3. 認証失敗時の要件を追加 | 2021/08/03 | 46F 垣屋 |
| | 3.3. 暗号鍵が漏洩しても他車両に影響しない鍵運用とする要件を追加 | | |
| | 3.3. パスワードに対する要件を追加 | | |
| | 3.3. 対象機器から受信したメッセージの検証失敗要件を追加 | | |
| | 3.3. Wi-Fi の Enterprise 採用時の認証要件を追加 | | |
| | 3.3. Bluetooth ペアリング機能の要件を追加 | | |
| | 3.4. サーバ認証失敗時の要件を追加 | | |
| | 3.4. セッション乗っ取りを回避する要件を追加 | | |
| | 3.4. クライアント認証に対称鍵を利用するケースにおいて、対称鍵を更新する要件を追加 | | |
| | 3.4. センターと車両間の通信経路の暗号化に利用する暗号鍵の更新要件を追加 | | |
| | 3.4. センターから受信したメッセージの検証要件要件を追加 | | |
| a00-02-a | 3.1. 「3.2. ファイアウォールに関する要求」と重複した要件を削除 | 2021/08/23 | 46F 垣屋 |
| | 3.1. TARA に紐づかない過剰な要件を削除 | | |
| | 3.1. DoS 攻撃発生した場合に、処理性能を維持する要件を明確化(2 つの要件 ID に分割) | | |
| | 3.3. 適用対象を正しく表現する記載に章題・要求を修正 | 2021/08/23 | 46F 清川 |
| a00-03-a | 章構成を変更 | 2021/09/02 | 46F 清川 |
| | WLSREQ_00206 要件の適用条件を追加 | | 46F 安江 |
| | WLSREQ_00540 要件の失効判断基準を追加 | | 46F 垣屋 |

| Version | 変更内容 | 日付 | 変更者 |
|---|---|---|---|
| | WLSREQ_00550 要件の適用条件と失効判断基準を追加 | | |
| a00-04-a | 要求一覧(2.5 章)の追加 | 2021/10/04 | 46F 安江 |
| | 要求の適用対象の明確化(3 章、WLSREQ_00203, WLSREQ_00205, WLSREQ_00209, WLSREQ_00410, WLSREQ_00490, WLSREQ_00530, WLSREQ_00540) | | |
| | 表現の明確化 (WLSREQ_00208, WLSREQ_00210) | 2021/10/07 | 46F 清川 |
| | 適用対象の明確化のために章/節のタイトル変更 (4.2.1 章、4.3.1.1 節、4.3.2.1 節) | 2021/10/12 | 46F 安江 |
| | 適用対象の明確化に合わせ、要求追加 ( WLSREQ_00611, WLSREQ_00371, WLSREQ_00372) | | |
| | 要件の明確化（WLSREQ_00460） | 2021/11/01 | 46F 清川 |
| | センターが対応する 2 アルゴリズムに対応するために、要件を変更（WLSREQ_00500） | 2021/11/01 | 46F 清川 |
| a00-05-a | ルート証明書の更新を削除 （WLSREQ_00500,WLSREQ_00510） | 2021/12/09 | 46F 石川 |
| a00-06-a | 日本語版の誤記修正 (WLSREQ_00210, WLSREQ_00311) 英語版の誤記修正 (WLSREQ_00317,WLSREQ_00318) | 2021/12/23 | 46F 石川 |
| a00-07-a | 要件の適用対象を修正 (WLSREQ_00317, WLSREQ_00611) | 2022/03/09 | 46F 清川 |
| | ICMP パケットに対する要件の明確化 (WLSREQ_00207) | 2022/03/09 | 46F 清川 |
| | 改ざん検知時の処理明確化（WLSREQ_00610, WLSREQ_00611, WLSREQ_00370, WLSREQ_00371, WLSREQ_00372) | 2022/03/09 | 46F 清川 |
| | センターに対する要求と ECU に対する要求に分割 保護対象の処理を明確化 (WLSREQ_00430, WLSREQ_00431, WLSREQ_00440, WLSREQ_00441) | 2022/03/09 | 46F 清川 |

| Version | 変更内容 | 日付 | 変更者 |
|---|---|---|---|
| | ルート証明書についての要求を修正<br>(WLSREQ_00500, WLSREQ_00520) | 2022/03/09 | 46F 清川 |
| | 補足の削除（WLSREQ_00360) | 2022/03/09 | 46F 清川 |
| | Bluetooth Security Check List の対応すべき項目の明確化（WLSREQ_00316) | 2022/03/09 | 46F 清川 |
| | クライアント認証に用いる秘密鍵・共通鍵の保管に関する要求を明確化（WLSREQ_00470) | 2022/03/10 | 46F 清川 |
| | 誤記修正 | 2022/03/11 | 46F 清川 |
| a00-08-a | 誤記修正 | 2022/05/20 | 46F 清川 |
| | 通信における大量のメッセージについて明確化<br>(WLSREQ_00120, WLSREQ_00130) | 2022/05/23 | 46F 清川 |
| | ファイアウォールに関する要求の明確化<br>（WLSREQ_00201, WLSREQ_00202, WLSREQ_00204） | 2022/06/02 | 46F 米谷 |
| | 関連文書の章構成の変更と公的関連文書の追加 | 2022/06/09 | 46F 安江 |
| | 証明書検証の明確化(WLSREQ_00540, WLSREQ_00550) | | |

# 目次

# 2. はじめに

## 2.1. 本書の目的

車外との無線通信時、通信内容の盗聴や改ざん、および、なりすましによる被害を防ぐため、通信路の保護、相互認証を行う。

本書では通信路の保護、相互認証の要件を定義する。

## 2.2. 適用範囲

本書の適用範囲は車外と直接無線通信を行う全ての ECU、及び、TLS 終端となる全ての ECU である。図 2-1 にその一部を示す。

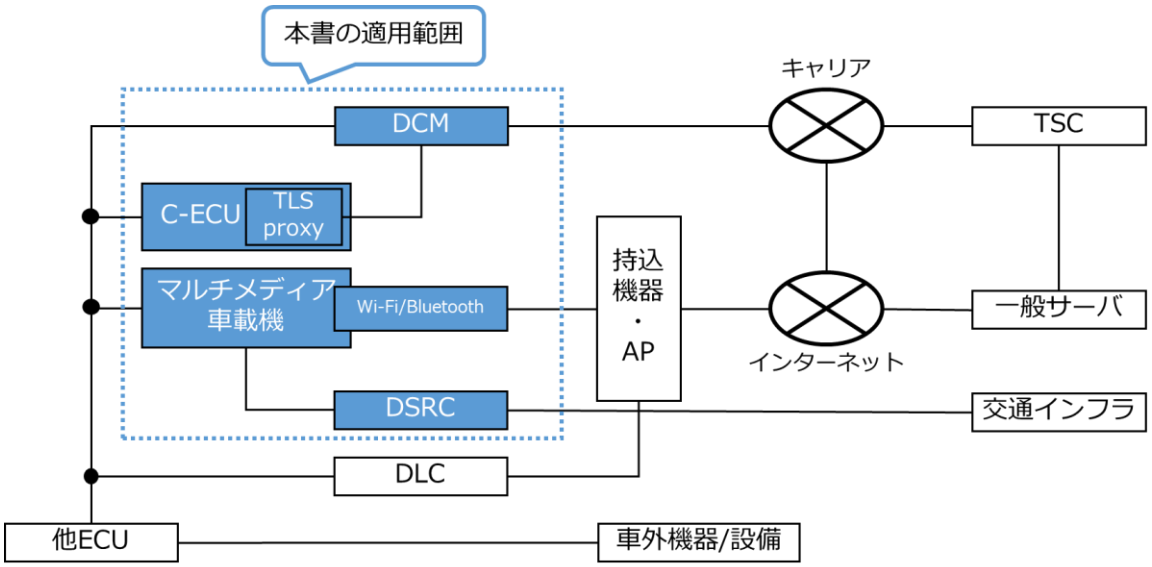



**図 2-1：本書の適用範囲**

## 2.3. 要求事項の記載

【WLSREQ_*****】と記載されている部分が本書で要求する仕様とする。ただし、（補足）と記載されているものは補足事項のため要求仕様ではない。

## 2.4. 上位文書

**表 2-1 上位文書一覧**

| No. | 文書名 | Ver.(最新版を適応ください) | 主管 |
|---|---|---|---|
| 1 | 車両サイバーセキュリティコンセプト定義書 | SEC-24PF-VCL-CPT-INST-DOC-***-**-* | 46F |

## 2.5. 関連文書

**表 2-2 関連文書一覧**

| No. | 文書名 | Ver.(最新版を適応ください) | 主管 |
|---|---|---|---|
| 1 | 共通脆弱性対策要求仕様書 | SEC-ePF-VUL-CMN-REQ-SPEC-a01-**-* | 46F |

**表 2-3 公的関連文書一覧**

| No. | 名称/外部リンク |
|---|---|
| 1 | RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2<br>https://www.ietf.org/rfc/rfc5246.txt |
| 2 | RFC8446: The Transport Layer Security (TLS) Protocol Version 1.3<br>https://www.ietf.org/rfc/rfc8446.txt |

# 3. 要求一覧

本書で規定する要求項目について、DoS 攻撃対策に関する要求一覧を表 3-1 に示す。ファイアウォールに関する要求一覧を表 3-2 に示す。認証・暗号化・改ざん検知のうち、センターに関する要求一覧を表 3-3 に示す。認証・暗号化・改ざん検知のうち、センター以外に関する要求一覧を表 3-4 に示す。要求事項の詳細については、4 章以降を参照。

また、ハードウェア選定時に参照すべき要求事項を「ハードウェア関連要求」列に「〇」で示す。

**表 3-1　DoS 攻撃対策に関する要求一覧**

| 分類 | 要求事項 | ハードウェア関連要求 | 適用対象 | |
|---|---|---|---|---|
| | | | サーバ | クライアント |
| 共通 | WLSREQ_00100 | - | 欠番 | |
| | WLSREQ_00110 | - | | |
| | WLSREQ_00120 | - | 〇 | 〇 |
| | WLSREQ_00130 | - | 〇 | 〇 |

**表 3-2　ファイアウォールに関する要求一覧**

| 分類 | 要求事項 | ハードウェア関連要求 | 適用対象 | |
|---|---|---|---|---|
| | | | サーバ | クライアント |
| IP 通信以外 | WLSREQ_00200 | - | ○ | ○ |
| IP 通信 | WLSREQ_00201 | - | ○ | ○ |
| | WLSREQ_00202 | - | ○ | ○ |
| | WLSREQ_00203 | - | - | ○ |
| | WLSREQ_00204 | - | 欠番 | |
| | WLSREQ_00205 | - | ○ | - |
| | WLSREQ_00206 | - | ○ | - |
| | WLSREQ_00207 | - | ○ | ○ |
| | WLSREQ_00208 | - | ○ | ○ |
| | WLSREQ_00209 | - | ○ | - |
| | WLSREQ_00210 | - | ○ | ○ |

**表 3-3　センターと接続する場合の認証・暗号化・改ざん検知に関する要求一覧**

| 分類 | 要求事項 | ハードウェア関連要求 | 適用対象 | |
|---|---|---|---|---|
| | | | サーバ | クライアント |
| TLS以外 | WLSREQ_00400 | - | ○ | ○ |
| | WLSREQ_00580 | - | ○ | ○ |
| | WLSREQ_00410 | - | - | ○ |
| | WLSREQ_00590 | - | ○ | ○ |
| | WLSREQ_00420 | - | ○ | ○ |
| | WLSREQ_00600 | - | ○ | ○ |
| | WLSREQ_00610 | - | ○ | ○ |
| TLS | WLSREQ_00121 | - | ○ | ○ |
| | WLSREQ_00122 | - | ○ | ○ |
| | WLSREQ_00401 | - | ○ | ○ |
| | WLSREQ_00402 | - | ○ | ○ |
| | WLSREQ_00411 | - | ○ | ○ |
| | WLSREQ_00430 | ○ | - | ○ |
| | WLSREQ_00431 | ○ | ○ | - |
| | WLSREQ_00440 | ○ | - | ○ |
| | WLSREQ_00441 | ○ | ○ | - |
| | WLSREQ_00450 | ○ | ○ | ○ |
| | WLSREQ_00460 | ○ | ○ | ○ |
| | WLSREQ_00470 | ○ | ○ | ○ |
| | WLSREQ_00480 | - | ○ | ○ |
| | WLSREQ_00490 | - | - | ○ |
| | WLSREQ_00500 | - | ○ | ○ |
| | WLSREQ_00510 | - | 欠番 | |
| | WLSREQ_00520 | - | ○ | ○ |
| | WLSREQ_00530 | ○ | ○ | - |
| | WLSREQ_00540 | - | - | ○ |
| | WLSREQ_00550 | - | ○ | - |
| | WLSREQ_00560 | - | ○ | ○ |
| | WLSREQ_00611 | - | - | ○ |

**表 3-4　センター以外の車外機器と接続する場合の認証・暗号化・改ざん検知に関する要求一覧**

| 分類 | 要求事項 | ハードウェア関連要求 | 適用対象 | |
|---|---|---|---|---|
| | | | サーバ※ | クライアント※ |
| Wi-Fi/ Bluetooth 以外 | WLSREQ_00300 | - | ○ | ○ |
| | WLSREQ_00350 | - | ○ | ○ |
| | WLSREQ_00360 | - | ○ | ○ |
| | WLSREQ_00310 | - | ○ | ○ |
| | WLSREQ_00370 | - | ○ | ○ |
| Wi-Fi | WLSREQ_00311 | - | ○ | ○ |
| | WLSREQ_00312 | - | ○ | ○ |
| | WLSREQ_00313 | - | ○ | ○ |
| | WLSREQ_00314 | - | ○ | ○ |
| | WLSREQ_00317 | - | ○ | - |
| | WLSREQ_00318 | - | ○ | ○ |
| | WLSREQ_00315 | - | ○ | ○ |
| | WLSREQ_00371 | - | ○ | ○ |
| Bluetooth | WLSREQ_00316 | - | ○ | ○ |
| | WLSREQ_00319 | - | ○ | ○ |
| | WLSREQ_00320 | - | ○ | ○ |
| | WLSREQ_00372 | - | ○ | ○ |

※Wi-Fi の場合、サーバ：アクセスポイント、クライアント：ステーションの意味

Bluetooth の場合、サーバ：マスタ、クライアント：スレーブの意味

# 4. 無線通信セキュリティ要求

以下に無線通信セキュリティ要求を以下に示す。

## 4.1. DoS 攻撃対策に関する要求

DoS 攻撃対策に関して、車外と直接または間接的に無線通信を行う ECU が適用する要件を以下に示す。

【要求事項：WLSREQ_00100】

（欠番）

【要求事項：WLSREQ_00110】

（欠番）

【要求事項：WLSREQ_00120】

システム/ECU 設計は、自 ECU が車外から以下に示す通信を受信する場合に、自 ECU として処理性能を維持すべき機能を特定すること

A） 実効スループットを実現する通信

B） 通信機能に割り当てられた ECU のリソース上限を消費する通信

(補足)自 ECU として処理性能を維持すべき機能を判断する基準は、システム/ECU 設計で決定する

【要求事項：WLSREQ_00130】

車外から以下に示す通信を受信したとき、WLSREQ_00120 で特定したそれぞれの機能の処理性能を維持できること

A） 実効スループットを実現する通信

B） 通信機能に割り当てられた ECU のリソース上限を消費する通信

対策例

－受信帯域幅を制限する

－通信に割り当てられたリソースを制限する

－通信に割り当てられたリソースと特定した機能に割り当てられたリソースを分離する

## 4.2. ファイアウォールに関する要求

ファイアウォールに関する要求を以下に示す。

### 4.2.1. IP 通信以外を使用する場合の要件

IP 通信以外を使用して車外と無線通信を行うエントリーポイント ECU が適用する要件を以下に示す。

【要求事項：WLSREQ_00200】

車外との通信は許可する通信のみを通信可能とし、不要な通信を遮断すること

### 4.2.2. IP 通信を使用する場合の要件

車外と無線で IP 通信を行うエントリーポイント ECU が適応する要件を以下に示す。

【要求事項：WLSREQ_00201】

使用しない TCP/UDP ポートは閉じておくこと。使用する TCP/UDP ポートは、サービス開始時・コネクション確立要求時に開け、サービス終了時・コネクション終了時に閉じること。

【要求事項：WLSREQ_00202】

確立中コネクションに関連するパケットのうち TCP 通信規則に従ったもののみ許可すること。TCP 通信規則に従わないものは遮断すること。

※対策例：シーケンス番号と確認応答番号の整合が取れたパケットのみ許容すること

【要求事項：WLSREQ_00203】

TCP 通信のサーバ機能を持たない場合は、車外からの TCP コネクション確立要求を棄却すること

【要求事項：WLSREQ_00204】

(欠番)

【要求事項：WLSREQ_00205】

TCP 通信のサーバ機能を有する場合は、 TCP 接続タイムアウト（3-way ハンドシェイクのタイムアウト）時間を、通信品質を満足できる範囲で最小化すること

【要求事項：WLSREQ_00206】

TCP 通信のサーバ機能を有する場合は、ハーフオープン状態（ACK を受信待ち）の TCP コネクションのデータでリソースが枯渇しないようにすること

※対策例：ACK を受信した契機でコネクションデータを生成/保持すること（TCP SYN cookies）

【要求事項：WLSREQ_00207】
全ての ICMP パケットを遮断すること。
全ての ICMP パケットを遮断できない場合は、以下のパケットを遮断すること。
- ICMP エコーリクエスト
- ECU 設計部署が受信することが必要と特定したタイプ/コード以外の ICMP パケット

【要求事項：WLSREQ_00208】
開けている TCP/UDP ポートは、単位時間当たりの許可される受信数を定義し、許容以上のパケットは破棄し、送信元への応答をしないこと
※対策例：Linux iptables や hashlimit

【要求事項：WLSREQ_00209】
TCP 通信のサーバ機能を有し、外部から TCP コネクションが確立されるポートがある場合は、同じ IP アドレスからの同時コネクション数を制限すること

【要求事項：WLSREQ_00210】
不要なブロードキャストアドレス宛のパケットは破棄し、送信元への応答をしないこと

## 4.3. 認証、暗号化、改ざん検知に関する要求

認証、暗号化、改ざん検知に関する要求を以下に示す。

### 4.3.1. センターと接続する場合の要求

センターや車外のサービスとの接続に関する要求を以下に示す。

#### 4.3.1.1. TLS 以外を用いる場合の要件

センターや車外のサービスと無線通信するエントリーポイント ECU が TLS 以外を用いる場合に適用する要件を以下に示す。

TLS については公的関連文書[1][2]参照。

【要求事項：WLSREQ_00400】

接続相手が不正なものでないことを確認するため認証を行うこと

認証が失敗した場合は、認証相手に応答をしないこと

【要求事項：WLSREQ_00580】

攻撃者によるセッション乗っ取り対策を実施すること

対策例：セッション ID の初期値を乱数で生成し推測困難性を確保する

【要求事項：WLSREQ_00410】

クライアント機能を有する場合は、センターサービスの不正利用防止を目的としたクライアント認証のための処理をサーバ接続時に行うこと。ただし、替わりに無線通信中継 ECU でクライアント認証のための処理を行ってもよい

【要求事項：WLSREQ_00590】

クライアント認証に対称鍵を使用する場合、機密性と完全性を担保してその対称鍵を更新または、切り替えできること

【要求事項：WLSREQ_00420】

車外のセンターやサービスへの接続時は通信路の暗号化、改ざん検知を行うこと。ただし、替わりに無線通信中継 ECU で通信路の暗号化、改ざん検知を行ってもよい

【要求事項：WLSREQ_00600】

通信経路の暗号化に使用する暗号鍵は、機密性と完全性を確保して更新できること

【要求事項：WLSREQ_00610】

センターより受信したメッセージの改ざんを検知した場合、当該メッセージを破棄し、センターへの応答をしないこと

#### 4.3.1.2. TLS を用いる場合の要件

無線通信で TLS の終端となるエントリーポイント ECU が適用する要件を以下に示す。
TLS については公的関連文書[1][2]参照。

【要求事項：WLSREQ_00121】
TLS 圧縮（TLS compression）機能を無効とすること

【要求事項：WLSREQ_00122】
TLS 再ネゴシエーション機能を無効とすること

【要求事項：WLSREQ_00401】
サーバ認証は TLS（バージョン 1.2 以上）標準のシーケンスに従って実施すること

【要求事項：WLSREQ_00402】
TLS 1.1 以下のバージョン（SSL を含む）を無効化すること

【要求事項：WLSREQ_00411】
トヨタセンター（トヨタサービス）との接続は、以下のいずれかの方式のクライアント認証のための処理を行うこと
—TLS（バージョン 1.2 以上）標準のシーケンス
—Appendix A に記載のシーケンス

【要求事項：WLSREQ_00430】
ECU はサーバ認証の署名検証処理を耐タンパ領域、もしくは、セキュア領域で行うこと（耐タンパ領域での処理を推奨）

【要求事項：WLSREQ_00431】
センターはサーバ認証の署名生成処理を耐タンパ領域、もしくは、セキュア領域で行うこと（耐タンパ領域での処理を推奨）

【要求事項：WLSREQ_00440】
ECU は以下の処理を耐タンパ領域で行うこと
・TLS 標準のシーケンスを採用した場合：クライアント認証の署名生成処理
・Appendix A に記載のシーケンスを採用した場合：クライアント認証符号(HMAC)の生成処理

【要求事項：WLSREQ_00441】
センターはクライアント認証の署名検証処理を耐タンパ領域、もしくは、セキュア領域で行うこと（耐タンパ領域での処理を推奨）

【要求事項：WLSREQ_00450】
公開鍵（ルート証明書等）は完全性を担保する領域へ保管すること

【要求事項：WLSREQ_00460】
クライアント認証に用いる秘密鍵・共通鍵は完全性、機密性が担保される耐タンパ領域へ保管すること

【要求事項：WLSREQ_00470】
キーストレージサイズの制約により、クライアント認証に用いる秘密鍵・共通鍵を耐タンパ性を有したハードウェア内へ保管することが困難である場合は、耐タンパ性を有したハードウェア内に保管した鍵を用いて暗号化、改ざん対策（認証子の付与など）を行った上で、耐タンパ性を有したハードウェアのみがアクセスできる領域に保管すること

【要求事項：WLSREQ_00480】
共有鍵、秘密鍵は情報漏洩無きよう鍵管理主管部署と協議の上、厳重に管理し運用すること

【要求事項：WLSREQ_00490】
クライアント機能を有する場合、クライアント認証鍵は車両毎にユニークとすること

【要求事項：WLSREQ_00500】
ルート証明書は下記の両方のアルゴリズムに対応し、ルート証明書の無効化ができること。
・ECDSA/256 bit 以上
・RSA/3072 bit 以上

【要求事項：WLSREQ_00510】
（欠番）

【要求事項：WLSREQ_00520】
ルート証明書無効化の完全性が担保されていること

【要求事項：WLSREQ_00530】
サーバ機能を有する場合、サーバ証明書の発行・更新を要求する際は既存の鍵情報は再利用せず、新たに公開鍵と秘密鍵の鍵ペアを生成すること

【要求事項：WLSREQ_00540】
クライアント機能を有する場合、サーバ認証時、以下の失効判断基準に従いサーバ証明書を検証し、失効している場合は認証しないこと
失効判断基準：
-証明書失効リスト(CRL)、もしくは OCSP による失効状態確認

【要求事項：WLSREQ_00550】
サーバ機能を有する場合は、クライアント認証を実施する際に、以下の失効判断基準に従いクライアント証明書を検証し、失効している場合は認証しないこと
失効判断基準：
-証明書失効リスト(CRL)、もしくは OCSP による失効状態確認

【要求事項：WLSREQ_00560】
車外のセンターとのサーバ認証時、中間 CA などを想定した多階層の認証に対応すること

【要求事項：WLSREQ_00611】
センターより受信したメッセージの改ざんを検知した場合、当該メッセージを破棄し、センターへの応答をしないこと

### 4.3.2. センター以外の車外機器と接続する場合の要求

センター以外の車外機器との接続に関する要求を以下に示す。

#### 4.3.2.1. Wi-Fi/Bluetooth 以外を用いる場合の要件

センター以外の車外機器と無線通信するエントリーポイント ECU が Wi-Fi/Bluetooth 以外を用いる場合に適用する要件を以下に示す。

【要求事項：WLSREQ_00300】
接続相手が不正なものでないことを確認するため認証を行うこと
認証が失敗した場合は、認証相手に応答をしないこと

【要求事項：WLSREQ_00350】
認証情報(ﾊﾟｽﾜｰﾄﾞ、暗号鍵等)は、漏洩時に他車両に影響しない認証情報とすること
※ 対策例：
-パスワード、及び暗号鍵は、各車載部品（シリアル No.毎）で個別とする
-公開鍵を利用する

【要求事項：WLSREQ_00360】
デフォルトのパスワードは、少なくとも数字、大文字、小文字を含み、長さを 8 桁以上とすること

【要求事項：WLSREQ_00310】
車外との接続時は通信路の暗号化、改ざん検知を行うこと

【要求事項：WLSREQ_00370】
車外から受信したメッセージの改ざんを検知した場合、当該メッセージを破棄し、送信元への応答をしないこと

#### 4.3.2.2. Wi-Fi を用いる場合の要件

車外機器と Wi-Fi で無線通信を行うエントリーポイント ECU が適応する要件を以下に示す。

【要求事項：WLSREQ_00311】
WPA2（Wi-Fi Protected Access 2）以降の規格を使用すること

【要求事項：WLSREQ_00312】
WPA3 をサポートしていること

【要求事項：WLSREQ_00313】
IEEE 802.11w をサポートしていること

【要求事項：WLSREQ_00314】
デフォルトの PSK（プリシェアドキー）は以下を満たすこと
・文字数が 13 文字以上であること
・パスワードには少なくとも数字、大文字、小文字を含めること
・各車載部品で個別とすること

【要求事項：WLSREQ_00317】
PSK をユーザが変更をする場合は以下を満たすこと
・文字数が 8 文字以上であること
・WLSREQ_00360 を満たせないパスワードが設定される場合、ユーザにリスクを提示すること

【要求事項：WLSREQ_00318】
WPA-Enterprise を利用する場合、WLSREQ_00350 に従った認証情報を使用すること

【要求事項：WLSREQ_00315】
SSID は空白及び、”ANY”以外とし、ECU 等の年代、製品名、及びパスワードを類推できないものとすること

【要求事項：WLSREQ_00371】
車外から受信したメッセージの改ざんを検知した場合、当該メッセージを破棄し、送信元への応答をしないこと

#### 4.3.2.3. Bluetooth を用いる場合の要件

車外機器と Bluetooth で無線通信を行うエントリーポイント ECU が適応する要件を以下に示す。

【要求事項：WLSREQ_00316】
Bluetooth を介した不正通信による車載機への侵入を防ぐために、Bluetooth 機能は NIST SP800-121（Bluetooth セキュリティ実装ガイド）に基づいて開発を行い、Bluetooth Security Check List の Recommended Practice 全項目に対応すること
（補足）Should consider の項目については任意
購入品である場合は、当該規格に基づいて開発された製品であることを確認すること。なお、暗号アルゴリズム要件などは SP800-121 References を参照すること

【要求事項：WLSREQ_00319】
車載 Bluetooth 機能は、SSP モード（Classic の場合）、もしくは LE Secure Connection モード(LE の場合)で外部デバイスとペアリングすること

【要求事項：WLSREQ_00320】
車載 Bluetooth 機能はペアリング要求に対して認証を行うこと

【要求事項：WLSREQ_00372】
車外から受信したメッセージの改ざんを検知した場合、当該メッセージを破棄し、送信元への応答をしないこと

# 5. Appendix A：セキュリティ機能のシーケンス

## 5.1. サーバ認証

サーバ認証シーケンスのサーバ認証準備パートを以下に示す。

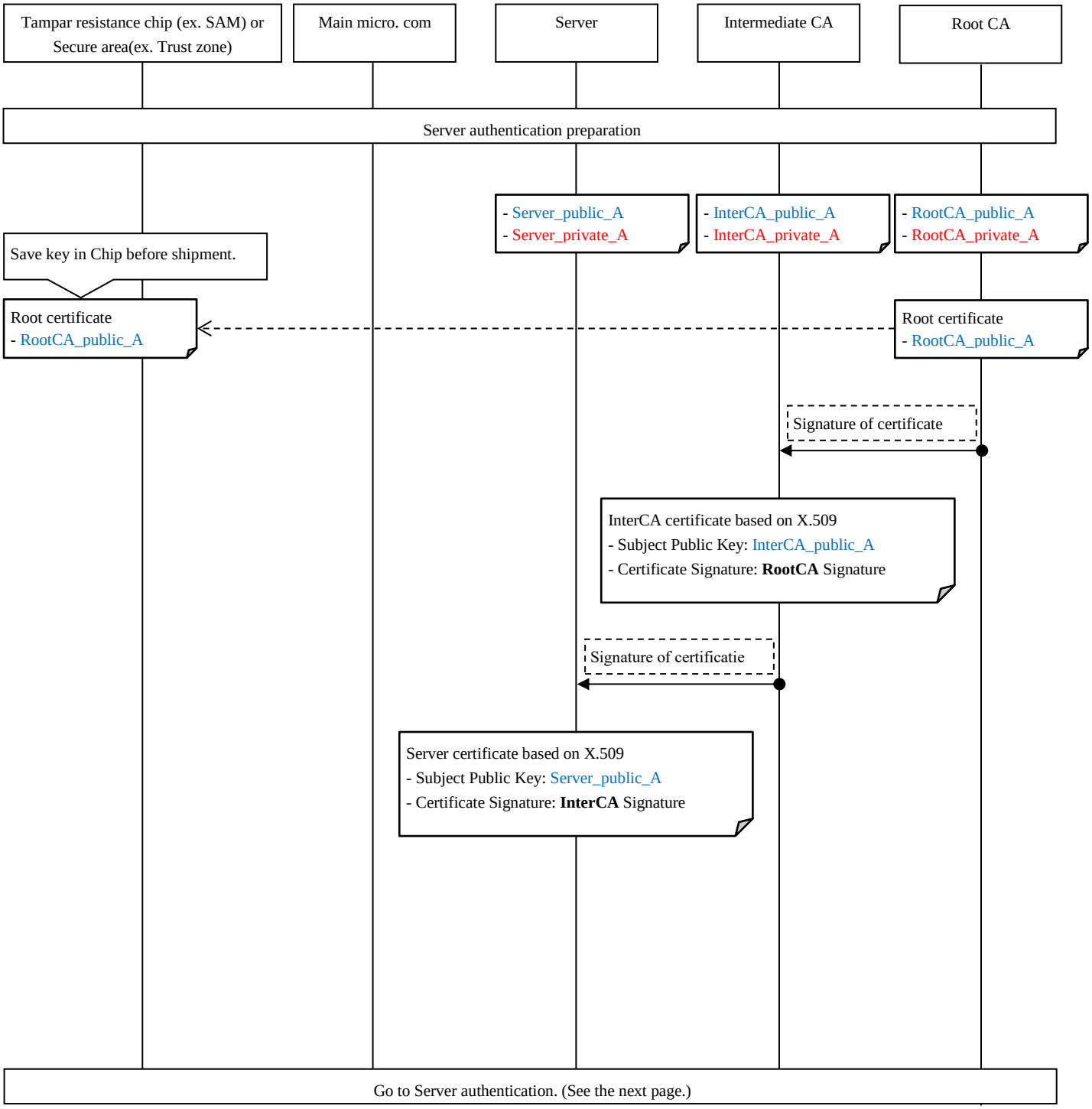



図 5-1 サーバ認証準備

サーバ認証シーケンスのサーバ認証パートを以下に示す。

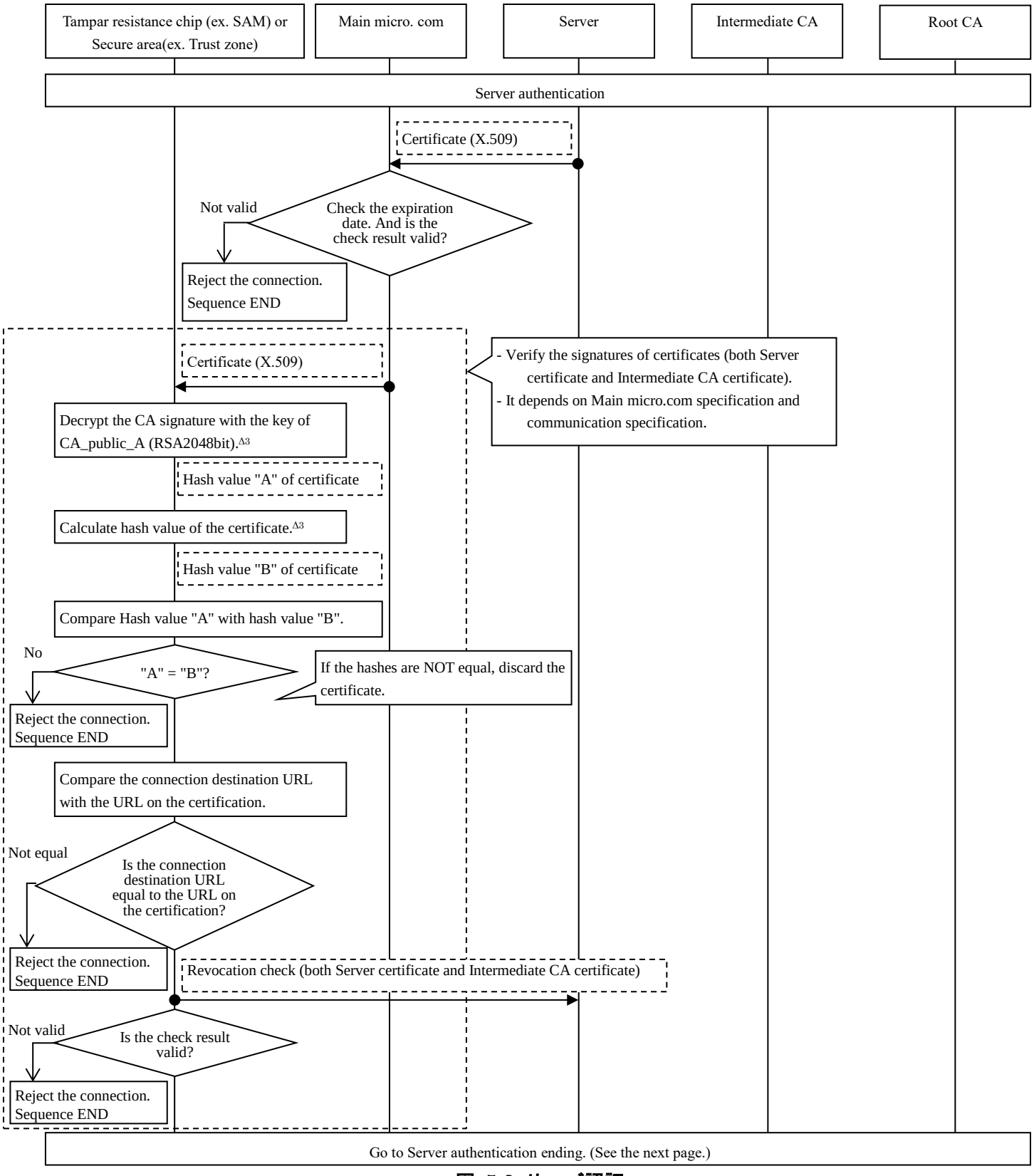



**図 5-2 サーバ認証**

サーバ認証シーケンスのサーバ認証終了パートを以下に示す。

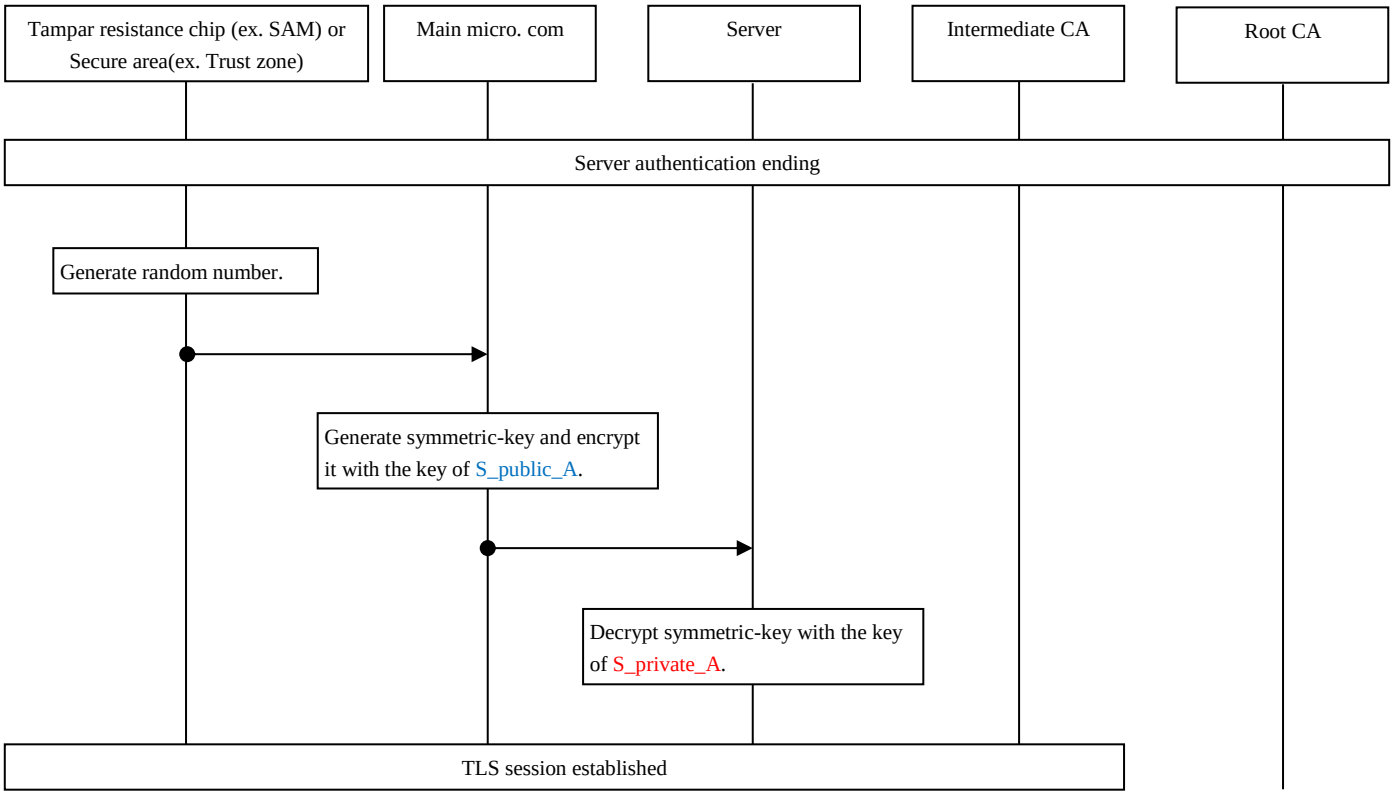



**図 5-3 サーバ認証終了**

## 5.2. クライアント認証

クライアント認証シーケンスを以下に示す。

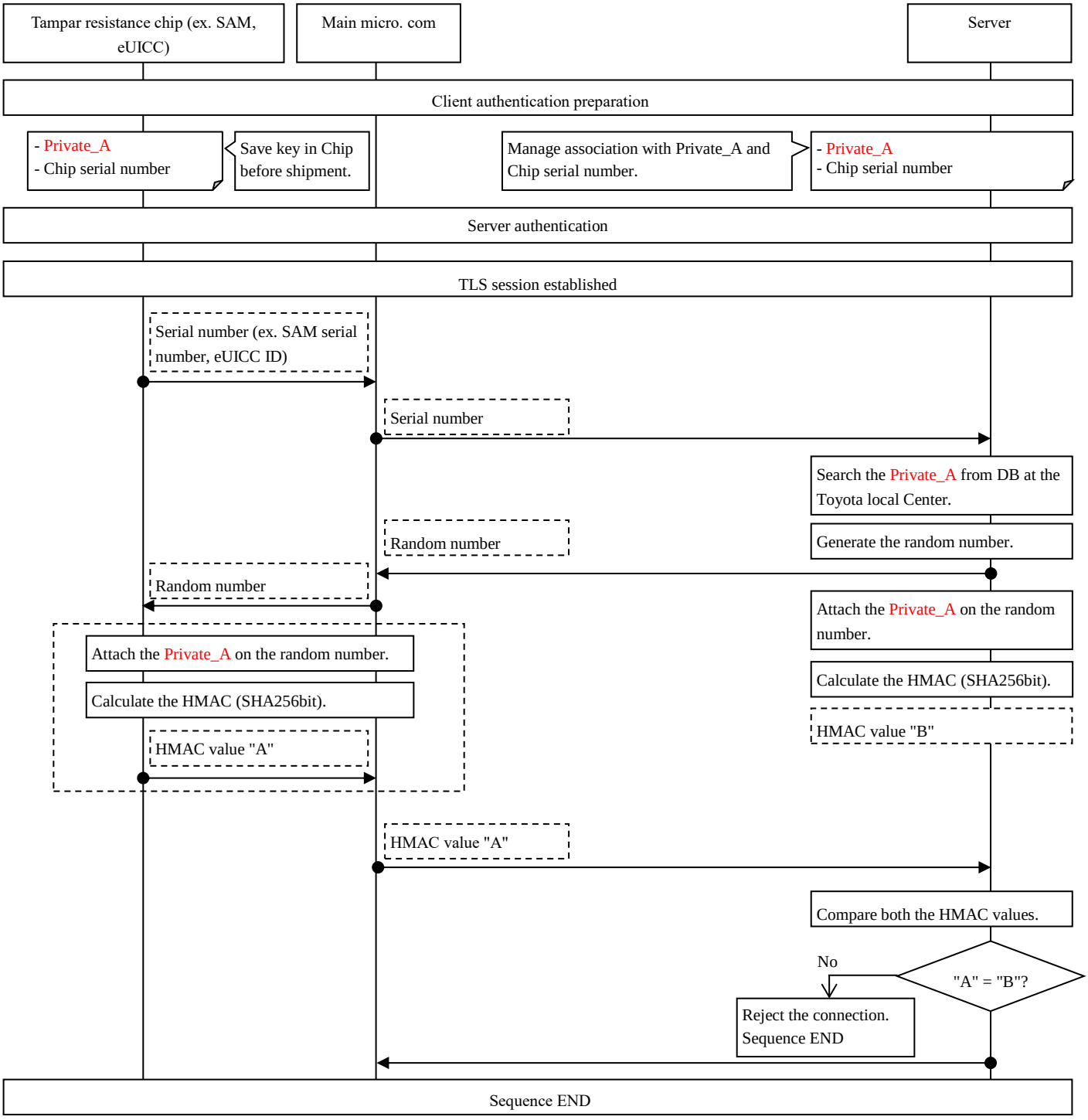



図 5-4 クライアント認証

# 1. Revision Record

| Version | Contents of revision | date | Changed by |
|---|---|---|---|
| a00-00-a | Initial Release | Apr. 01,2021 | 46F Kakiya |
| a00-00-b | Add English translation | May 31,2021 | 46F Kiyokawa |
| | Delete the section “2.5 Terms and Definitions”, because Terms related to Cybersecurity are described in SEC-ePF-TRM-GUD-PROC-***-**-*. | ↑ | ↑ |
| | Correct requirement ID errors.<br>(Requirement number is not changed.)<br>WSECR_***** ⇒ WLSREQ_***** | ↑ | ↑ |
| | Clarify the upper-level documents | ↑ | ↑ |
| | Add Appendix A. | ↑ | ↑ |
| a00-01-a | 3.3. Add the requirement when an authentication fails. | Aug. 03,2021 | 46F Kakiya |
| | 3.3. Add the requirement of key management that cryptographic keys do not affect other vehicles in case of leakage. | ↑ | ↑ |
| | 3.3. Add the requirement of password | ↑ | ↑ |
| | 3.3. Add the requirement when a received message from a target device verification fails. | ↑ | ↑ |
| | 3.3. Add the requirement of authentication for Wi-Fi enterprise. | ↑ | ↑ |
| | 3.3. Add the requirement of Bluetooth pairing function. | ↑ | ↑ |
| | 3.4. Add the requirement when server authentication fails. | ↑ | ↑ |
| | 3.4. Add the requirement to prevent session hijacking. | ↑ | ↑ |
| | 3.4. Add the requirement to update a symmetric key if a symmetric key is used for client authentication. | ↑ | ↑ |
| | 3.4. Add the requirement to update an encryption key that is used to encrypt communications between a center and a vehicle. | ↑ | ↑ |
| | 3.4. Add the requirement when message verification fails. | ↑ | ↑ |

| | | | |
|---|---|---|---|
| a00-02-a | 3.1. Delete the requirement duplicated with “3.2. Requirements related to Firewall”. | Aug. 23,2021 | 46F Kakiya |
| | 3.1. Delete the requirement that are not tied to TARA. | ↑ | ↑ |
| | 3.1 Clarify the requirement to remain processing performance when DoS attack occurs.(divided into two requirements). | ↑ | ↑ |
| | 3.3. Clarify expressions of the section title and requirements to properly express scope of requirement. | Aug. 23,2021 | 46F Kiyokawa |
| a00-03-a | Change chapter structure | Sep. 02,2021 | 46F Kiyokawa |
| | WLSREQ_00206<br>Add apply condition. | | 46F Yasue |
| | WLSREQ_00540<br>Add the certificate revocation criteria. | | 46F Kakiya |
| | WLSREQ_00550<br>Add the apply condition and the certificate revocation criteria. | | |
| a00-04-a | Add chapter 3 ‘Outline of Requirements’ | Oct. 04,2021 | 46F Yasue |
| | Clarify the applicable target of requirements (section 3, WLSREQ_00203, WLSREQ_00205, WLSREQ_00209, WLSREQ_00410, WLSREQ_00490, WLSREQ_00530, WLSREQ_00540) | | |
| | Clarify expressions.<br>(WLSREQ_00208, WLSREQ_00210) | Oct. 07,2021 | 46F Kiyokawa |
| | Change title of chapter and section to clarify the applicable target (chapter 4.2.1, section 4.3.1.1 and 4.3.2.1) | Oct. 12,2021 | 46F Yasue |
| | Add requirements in accordance with clarification of the above applicable target (WLSREQ_00611, WLSREQ_00371, WLSREQ_00372) | | |
| | Clarify the requirement. (WLSREQ_00460) | Nov. 01,2021 | 46F Kiyokawa |

| | | | |
|---|---|---|---|
| | Change the requirement to support two algorithms that center support. (WLSREQ_00500) | Nov. 01,2021 | 46F Kiyokawa |
| a00-05-a | Delete Root Certificate updating. (WLSREQ_00500, WLSREQ_00510) | Dec. 09,2021 | 46F Ishikawa |
| a00-06-a | Correct errors in the Japanese version (WLSREQ_00210, WLSREQ_00311) Correct errors in the English version (WLSREQ_00317, WLSREQ_00318) | Dec. 23,2021 | 46F Ishikawa |
| a00-07-a | Modify the applicable target of the requirement (WLSREQ_00317) | Mar. 09,2022 | 46F Kiyokawa |
| | Clarify the requirement for ICMP packets (WLSREQ_00207) | Mar. 09,2022 | 46F Kiyokawa |
| | Clarify the processing when a tampering is detected (WLSREQ_00610, WLSREQ_00611, WLSREQ_00370, WLSREQ_00371, WLSREQ_00372) | Mar. 09,2022 | 46F Kiyokawa |
| | Separate each requirement into a requirement to the center and a requirement to the ECU. Clarify the processing to be protected (WLSREQ_00430, WLSREQ_00431, WLSREQ_00440, WLSREQ_00441) | Mar. 09,2022 | 46F Kiyokawa |
| | Modify requirements related to root certificate (WLSREQ_00500, WLSREQ_00520) | Mar. 09,2022 | 46F Kiyokawa |
| | Delete the supplement (WLSREQ_00360) | Mar. 09,2022 | 46F Kiyokawa |
| | Clarify the items to be supported in Bluetooth Security Check List (WLSREQ_00316) | Mar. 09,2022 | 46F Kiyokawa |
| | Clarify the requirement to store private key and symmetric key for client authentication (WLSREQ_470) | Mar, 10,2022 | 46F Kiyokawa |
| | Correct editorial errors | Mar. 11,2022 | 46F Kiyokawa |
| a00-08-a | Correct editorial errors | May. 20,2022 | 46F Kiyokawa |
| | Clarify a large number of messages in terms of communication (WLSREQ_00120, WLSREQ_00130) | May. 23,2022 | 46F Kiyokawa |

| | | | |
|---|---|---|---|
| | Clarify the requirement related to firewall (WLSREQ_00201, WLSREQ_00202, WLSREQ_00204) | Jun. 2,2022 | 46F Komedani |
| | Change the section structure for related document and add Public Related Documents | Jun. 9, 2022 | 46F Yasue |
| | Clarify the Certificate verification (WLSREQ_00540, WLSREQ_00550) | | |

# Table of Contents

# 2. Introduction

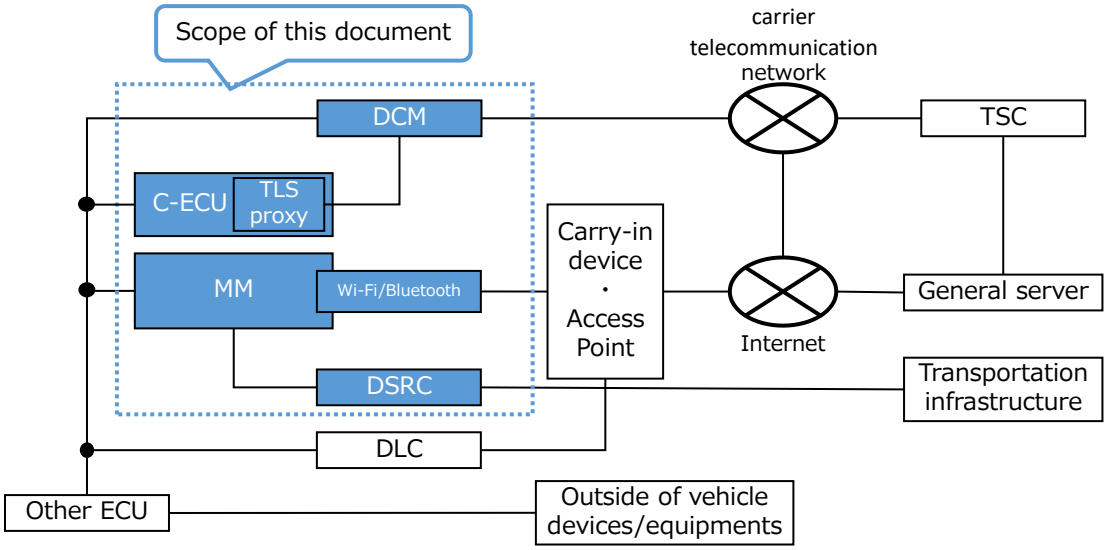
## 2.1. Purpose of This Document

When the ECU communicate wirelessly with outside target of the vehicle, the ECU protects communication channel and authenticates mutually, in order to prevent eavesdropping, tampering and spoofing of communication data.

This document defines the requirements of communication channel protection and mutual authentication.

## 2.2. Scope of This Document

The scope of this document is every ECU that communicate directly with outside target of the vehicle using wireless communication protocol and every TLS terminal ECU. In "**エラー! 参照元が見つかりません。**", a part of it is shown.




## 2.3. Description of Requirements

A requirement in this document shall be labeled as 【WLSREQ_*****】. Provided, however, that what is labeled as (Supplement) in 【WLSREQ_*****】 is a supplementary item and therefore is not a requirement specification.

## 2.4. Upper-level Documents

**Table 2-1 Upper-level Documents**

| No. | Title | Ver.(See the latest version) | Issued |
|---|---|---|---|
| 1 | Vehicle Cybersecurity Concept Definition | SEC-24PF-VCL-CPT-INST-DOC-***-**-* | 46F |

## 2.5. Related Documents

**Table 2-2 Related Documents**

| No. | Title | Ver.(See the latest version) | Issued |
|---|---|---|---|
| 1 | Requirements Specification of Common Vulnerability Countermeasure | SEC-ePF-VUL-CMN-REQ-SPEC-a01-**-* | 46F |

**Table 2-3 Public Related Documents**

| No. | Title and External link |
|---|---|
| 1 | RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2<br>https://www.ietf.org/rfc/rfc5246.txt |
| 2 | RFC8446: The Transport Layer Security (TLS) Protocol Version 1.3<br>https://www.ietf.org/rfc/rfc8446.txt |

# 3. List of Requirements

For the requirement items defined in this document, list of requirement items related to the countermeasure against DoS attacks are shown in Table 3-1. List of requirement items related to Firewall are shown in Table 3-2. List of requirement items related to authentication, encryption and tamper detection with Center are shown in Table 3-3. List of requirement items related to authentication, encryption and tamper detection with devices outside of vehicle except for center are shown in Table 3-4.

The requirements to which ECU designer should refer in selecting hardware are marked with "○" in the "Hardware-related requirements" column.

**Table 3-1 Requirements list related to the countermeasure against DoS attacks**

| Classification | Requirement | Hardware-Related Requirements | Applicable target | |
|---|---|---|---|---|
| | | | Server | Client |
| Common | WLSREQ_00100 | - | Deleted | |
| | WLSREQ_00110 | - | | |
| | WLSREQ_00120 | - | ○ | ○ |
| | WLSREQ_00130 | - | ○ | ○ |

**Table 3-2 Requirements list related to Firewall**

| Classification | Requirement | Hardware-Related Requirements | Applicable target | |
|---|---|---|---|---|
| | | | Server | Client |
| Except for IP communication | WLSREQ_00200 | - | ○ | ○ |
| IP communication | WLSREQ_00201 | - | ○ | ○ |
| | WLSREQ_00202 | - | ○ | ○ |
| | WLSREQ_00203 | - | - | ○ |
| | WLSREQ_00204 | - | Deleted | |
| | WLSREQ_00205 | - | ○ | - |
| | WLSREQ_00206 | - | ○ | - |
| | WLSREQ_00207 | - | ○ | ○ |
| | WLSREQ_00208 | - | ○ | ○ |
| | WLSREQ_00209 | - | ○ | - |
| | WLSREQ_00210 | - | ○ | ○ |

**Table 3-3 Requirements list related to authentication, encryption and tamper detection in the case of connecting with Center**

| Classification | Requirement | Hardware-Related Requirements | Applicable target | |
|---|---|---|---|---|
| | | | Server | Client |
| Except for TLS | WLSREQ_00400 | - | ○ | ○ |
| | WLSREQ_00580 | - | ○ | ○ |
| | WLSREQ_00410 | - | - | ○ |
| | WLSREQ_00590 | - | ○ | ○ |
| | WLSREQ_00420 | - | ○ | ○ |
| | WLSREQ_00600 | - | ○ | ○ |
| | WLSREQ_00610 | - | ○ | ○ |
| TLS | WLSREQ_00121 | - | ○ | ○ |
| | WLSREQ_00122 | - | ○ | ○ |
| | WLSREQ_00401 | - | ○ | ○ |
| | WLSREQ_00402 | - | ○ | ○ |
| | WLSREQ_00411 | - | ○ | ○ |
| | WLSREQ_00430 | ○ | - | ○ |
| | WLSREQ_00431 | ○ | ○ | - |
| | WLSREQ_00440 | ○ | - | ○ |
| | WLSREQ_00441 | ○ | ○ | - |
| | WLSREQ_00450 | ○ | ○ | ○ |
| | WLSREQ_00460 | ○ | ○ | ○ |
| | WLSREQ_00470 | ○ | ○ | ○ |
| | WLSREQ_00480 | - | ○ | ○ |
| | WLSREQ_00490 | - | - | ○ |
| | WLSREQ_00500 | - | ○ | ○ |
| | WLSREQ_00510 | - | Deleted | |
| | WLSREQ_00520 | - | ○ | ○ |
| | WLSREQ_00530 | ○ | ○ | - |
| | WLSREQ_00540 | - | - | ○ |
| | WLSREQ_00550 | - | ○ | - |
| | WLSREQ_00560 | - | ○ | ○ |
| | WLSREQ_00611 | - | - | ○ |

**Table 3-4 Requirements list related to authentication, encryption and tamper detection in the case of connecting with devices outside of vehicle except for center**

| Classification | Requirement | Hardware-Related Requirements | Applicable target | |
|---|---|---|---|---|
| | | | Server(*) | Client(*) |
| Except for Wi-Fi/Bluetooth | WLSREQ_00300 | - | ○ | ○ |
| | WLSREQ_00350 | - | ○ | ○ |
| | WLSREQ_00360 | - | ○ | ○ |
| | WLSREQ_00310 | - | ○ | ○ |
| | WLSREQ_00370 | - | ○ | ○ |
| Wi-Fi | WLSREQ_00311 | - | ○ | ○ |
| | WLSREQ_00312 | - | ○ | ○ |
| | WLSREQ_00313 | - | ○ | ○ |
| | WLSREQ_00314 | - | ○ | ○ |
| | WLSREQ_00317 | - | ○ | - |
| | WLSREQ_00318 | - | ○ | ○ |
| | WLSREQ_00315 | - | ○ | ○ |
| | WLSREQ_00371 | - | ○ | ○ |
| Bluetooth | WLSREQ_00316 | - | ○ | ○ |
| | WLSREQ_00319 | - | ○ | ○ |
| | WLSREQ_00320 | - | ○ | ○ |
| | WLSREQ_00372 | - | ○ | ○ |

(*) In case of Wi-Fi, Server means Access point and then Client means Station.

In case of Bluetooth, Server means Master and then Client means Slave.

# 4. Wireless Communication Security Requirements

This chapter defines wireless communication security requirements.

## 4.1. Requirements related to Countermeasures against DoS Attack

The following requirements about countermeasure against DoS attack are applied to an ECU that wirelessly communicates directly or indirectly with target outside of the vehicle.

【Requirement ID: WLSREQ_00100】

(Deleted)

【Requirement ID: WLSREQ_00110】

(Deleted)

【Requirement ID: WLSREQ_00120】

System/ECU design department shall define own ECU's functions that have to be remained a certain processing performance when the ECU receives the following communication from outside of the vehicle.

A) communication that achieves effective throughput
B) communication that exhausts the upper limit of the resource in ECU allocated for the communication function

(supplement) System/ECU design department may determine the criteria to determine own ECU's functions that have to be remained a certain processing performance.

【Requirement ID: WLSREQ_00130】

When an ECU receives the following communication from outside of the vehicle, the ECU shall remain the certain processing performance of each defined function.

A) communication that achieves effective throughput
B) communication that exhausts the upper limit of the resource in ECU allocated for the communication function

(Examples of countermeasure)

- Limit the receiver bandwidth
- Limit the resource allocated for the communication
- Separate the resource allocated for the communication and the resource allocated for each defined function

## 4.2. Requirements related to Firewall

Requirements about firewall are indicated below.

### 4.2.1. Requirements for using except for IP Communication

The following requirements are applied to an entry point ECU that uses except for IP communication wirelessly with target outside of the vehicle.

【Requirement ID: WLSREQ_00200】

The ECU shall permit only permitted communication and discard unnecessary communication in communication with outside of vehicle.

### 4.2.2. Requirements for using IP Communication

The following requirements are applied to an entry point ECU that uses IP communication wirelessly with target outside of the vehicle.

【Requirement ID: WLSREQ_00201】

The ECU shall close the TCP/UDP port not to be used. The ECU shall open the TCP/UDP port to be used when an associated service starts or the ECU requests connection establishment, and the ECU shall close the port when the service finishes or the ECU terminates connection.

【Requirement ID: WLSREQ_00202】

The ECU shall permit only packets that comply with TCP protocol out of the packets that are communicated in established connection. The ECU shall discard packets that do not comply with TCP protocol.
※Example of countermeasures：Only permit packets that are consistent of sequence number and acknowledgement number.

【Requirement ID: WLSREQ_00203】

If the ECU does not have server function on TCP communication, if TCP connection establishment from outside of vehicle are not permitted, the ECU shall discard the TCP connection establishment request.

【Requirement ID: WLSREQ_00204】

(Deleted)

【Requirement ID: WLSREQ_00205】

If the ECU has server function on TCP communication, the ECU shall minimize TCP connection timeout period (timeout of 3-way handshake) within the range that satisfies communication quality.

【Requirement ID: WLSREQ_00206】

If the ECU has server function on TCP communication, the ECU shall not exhaust resources due to the data

related to TCP connection in half-open status (Waiting for ACK to be received)

※Example of countermeasure：Generate/maintain connection data upon receipt of an ACK. (TCP SYN cookies)

【Requirement ID: WLSREQ_00207】

The ECU shall discard all ICMP packets.

If the ECU cannot discard all ICMP packets, the ECU shall discard packets indicated below.

- ICMP echo request.
- ICMP packets other than the types/codes that the ECU design department determines necessary to be received.

【Requirement ID: WLSREQ_00208】

The ECU shall define the permitted number of packets received per unit time for open TCP/UDP ports.
In addition, the ECU shall drop the packets and shall not respond to the sender if the permitted number is exceeded.

※Example of countermeasure：Linux iptables or hashlimit

【Requirement ID: WLSREQ_00209】

If the ECU has server function on TCP communication, if there are ports that TCP connection are established from outside of vehicle, the ECU shall limit the number of simultaneous connections from same IP address.

【Requirement ID: WLSREQ_00210】

The ECU shall drop the packets addressed to an unnecessary broadcast address and shall not respond to the sender.

## 4.3. Requirements for Authentication, Encryption and Tamper Detection

Requirements about authentication, encryption, and tamper detection are indicated below.

### 4.3.1. Requirements related to connection with center

Requirements related to connection with center or service outside of vehicle are indicated below.

#### 4.3.1.1. Requirements for using except for TLS Communication

The following requirements are applied to an entry point ECU that uses except for TLS communication wirelessly with center or service outside of vehicle.

About TLS, refer to Public Related Documents[1][2].

【Requirement ID: WLSREQ_00400】

When connecting, the ECU shall authenticate the server to prevent the connection with malformed center.

If the server authentication fails, the ECU shall not respond to the center.

【Requirement ID: WLSREQ_00580】

The ECU shall prevent session hijacking by attackers.

E.g.- Generate the initial value of the session ID in random numbers to make it difficult to guess.

【Requirement ID: WLSREQ_00410】

If the ECU has client function, when connecting with server, the ECU shall perform operations for client authentication to prevent unauthorized use of center service. Alternatively, Wireless communication gateway ECU may perform operations for client authentication.

【Requirement ID: WLSREQ_00590】

If the ECU uses a symmetric key for client authentication, the symmetric key shall be updated or switched in the way to ensure its integrity and confidentiality.

【Requirement ID: WLSREQ_00420】

When connecting with outside of vehicle center or service, the ECU shall encrypt the channel and detect tampering.

Alternatively, Wireless communication gateway ECU may encrypt the channel and detect tampering.

【Requirement ID: WLSREQ_00600】

An encryption key used to encrypt a channel shall be updated in the way to ensure its integrity and confidentiality.

【Requirement ID: WLSREQ_00610】

If the ECU detects a tampering of the received message from center, the ECU shall drop the messages and shall not respond to the center.

#### 4.3.1.2. **Requirements for using TLS Communication**

The following requirements are applied to an entry point ECU that is TLS terminal in wireless communication. About TLS, refer to Public Related Documents[1][2].

【Requirement ID: WLSREQ_00121】

The ECU shall disable the TLS compression function.

【Requirement ID: WLSREQ_00122】

The ECU shall disable the TLS renegotiation function.

【Requirement ID: WLSREQ_00401】

The ECU shall perform server authentication complying with TLS standard sequence. (version 1.2 or later)

【Requirement ID: WLSREQ_00402】

TLS 1.1 or the earlier versions (which include SSL) shall be disabled for vulnerability countermeasures.

【Requirement ID: WLSREQ_00411】

When the ECU connects with Toyota center (Toyota service), the ECU shall perform processing for client authentication in one of the following ways.

—TLS (version 1.2 or later) standard sequence.

—The sequence described in Appendix A.

【Requirement ID: WLSREQ_00430】

The ECU shall process the signature verification for server authentication in anti-tampering area or secure area. (processing in anti-tampering area is recommended)

【Requirement ID: WLSREQ_00431】

The center shall process the signature generation for server authentication in anti-tampering area or secure area. (processing in anti-tampering area is recommended)

【Requirement ID: WLSREQ_00440】

The ECU shall process operations indicated below in anti-tampering area.

・In the case that TLS standard sequence is used: signature generation for client authentication.

・In the case that the sequence described in Appendix A is used: generation for client authentication code (HMAC)

【Requirement ID: WLSREQ_00441】

The center shall process the signature verification for client authentication in anti-tampering area or secure area. (processing in anti-tampering area is recommended)

【Requirement ID: WLSREQ_00450】

Public key（e.g. Root Certificate）shall be stored in the area ensured integrity.

【Requirement ID: WLSREQ_00460】

Private key and symmetric key used for client authentication shall be stored in anti-tampering area ensured integrity and confidentiality.

【Requirement ID: WLSREQ_00470】

If it is difficult for the ECU to store private key and symmetric key for client authentication in anti-tampering hardware due to the limitation of key storage size, the ECU shall perform encryption and countermeasures against tampering (giving an authentication code, etc.) for the keys using a key stored in anti-tampering hardware and shall store the keys in an area where only the anti-tampering hardware can access.

【Requirement ID: WLSREQ_00480】

Private key and symmetric key shall be strictly managed and operated in consultation with the administration department of key management in order to prevent any key information leakage.

【Requirement ID: WLSREQ_00490】

If the ECU has client function, client authentication key shall be unique in each vehicle.

【Requirement ID: WLSREQ_00500】

The ECU shall support both algorithms below for Root Certificates, and the ECU shall be able to disable the Root Certificates.

・ECDSA/256 bits or more

・RSA/3072 bits or more

【Requirement ID: WLSREQ_00510】

(Deleted)

【Requirement ID: WLSREQ_00520】

Integrity of Root Certificate disabling shall be ensured.

【Requirement ID: WLSREQ_00530】

If the ECU has server function, when the ECU requests issuing and updating a Server Certificate, the ECU shall not reuse current key information in ECU and generate a new private and public key pair for it.

【Requirement ID: WLSREQ_00540】

If the ECU has client function, when the ECU authenticates the server, the ECU shall verify Server Certificate in accordance with the following certificate revocation criteria. In addition, the ECU shall not authenticate the server if it has been invalid.

Certificate revocation criteria:

-Revocation status confirmation by Certificate Revocation List (CRL) or OCSP.

【Requirement ID: WLSREQ_00550】

If the ECU has server function, when the ECU authenticates the client, the ECU shall verify Client Certificate in accordance with the following certificate revocation criteria. In addition, the ECU shall not authenticate the client if it has been invalid.

Certificate revocation criteria:

-Revocation status confirmation by Certificate Revocation List (CRL) or OCSP.

【Requirement ID: WLSREQ_00560】

If the ECU authenticate a center outside of vehicle, server authentication shall support multi-layered authentication such as using intermediate CA.

【Requirement ID: WLSREQ_00611】

If the ECU detects a tampering of the received message from center, the ECU shall drop the messages and shall not respond to the center.

### 4.3.2. Requirements related to Connection with Devices outside of vehicle except for Center

Requirements related to connection with devices outside of vehicle except for center are indicated below.

#### 4.3.2.1. Requirements for using except for Wi-Fi/Bluetooth

The following requirements are applied to an entry point ECU that uses except for Wi-Fi/Bluetooth communicates wirelessly with devices outside of vehicle except for Center.

【Requirement ID: WLSREQ_00300】

The ECU shall authenticate each connection counterparts to confirm that it is not malformed.
If the authentication fails, the ECU shall not respond to the authentication counterpart.

【Requirement ID: WLSREQ_00350】

The confidential information, e.g. password, encryption key, shall not affect other vehicles in case of leakage.
E.g. - Passwords or encryption keys are separated for each in-vehicle part (each serial no.).
- Using a public key.

【Requirement ID: WLSREQ_00360】

The default password set by string shall contain at least numbers, uppercase letters and lowercase letters, and shall be at least 8 digits in length.

【Requirement ID: WLSREQ_00310】

When the ECU connects with outside of the vehicle, the ECU shall encrypt the channel and detect tampering.

【Requirement ID: WLSREQ_00370】

If the ECU detects a tampering of the received message from outside of the vehicle, the ECU shall drop the messages and shall not respond to the sender.

#### 4.3.2.2. Requirements for using Wi-Fi

The following requirements are applied to an entry point ECU that communicates wirelessly with devices outside of vehicle using Wi-Fi.

【Requirement ID: WLSREQ_00311】

The ECU shall use WPA2（Wi-Fi Protected Access 2） and later.

【Requirement ID: WLSREQ_00312】

The ECU shall support WPA3.

【Requirement ID: WLSREQ_00313】

The ECU shall support IEEE 802.11w.

【Requirement ID: WLSREQ_00314】

The default PSK（Pre-Shared Key）shall satisfy the following

・The number of character string is 13 and more.

・The password set by string consists at least number, uppercase letters and lowercase letters.

・Separate for each in-vehicle part, each serial No.

【Requirement ID: WLSREQ_00317】

When a user changes the default PSK, it shall satisfy the followings

・The number of character string is 8 and more.

・If the user change to a password which does not satisfy WLSREQ_00360, the ECU notifies the risk of it.

【Requirement ID: WLSREQ_00318】

If the ECU uses WPA-Enterprise, the ECU shall use the confidential information in accordance with WLSREQ_00350.

【Requirement ID: WLSREQ_00315】

SSID shall be set to the value other than blank and “ANY”, and that the value cannot analogize the password and product name, age of ECU and so on.

【Requirement ID: WLSREQ_00371】

If the ECU detects a tampering of the received message from outside of the vehicle, the ECU shall drop the messages and shall not respond to the sender.

#### 4.3.2.3. **Requirements for using Bluetooth**

The following requirements are applied to an entry point ECU that communicates wirelessly with devices outside of vehicle using Bluetooth.

【Requirement ID: WLSREQ_00316】

Bluetooth function shall be developed based on NIST SP800-121 (Guide to Bluetooth Security) and shall support all Recommended Practice items in Bluetooth Security Check List in order to prevent intrusion to in-vehicle devices due to unauthorized communication using Bluetooth.

If the Bluetooth function is a purchased product, it shall be confirmed that the product is developed based on the above relevant standard.

In addition, refer SP800-121 References for requirements of encryption algorism and so on.

【Requirement ID: WLSREQ_00319】

In-vehicle Bluetooth function of the ECU shall pair external devices using SSP mode (in case of Classic) or LE Secure Connection mode (in case of LE).

【Requirement ID: WLSREQ_00320】

In-vehicle Bluetooth function of the ECU shall authenticate the Bluetooth pairing request.

【Requirement ID: WLSREQ_00372】

If the ECU detects a tampering of the received message from outside of the vehicle, the ECU shall drop the messages and shall not respond the sender.

# 5. Appendix A: The sequence of information security function

## 5.1. Server Authentication

The part of server authentication preparation of server authentication sequence is shown below.

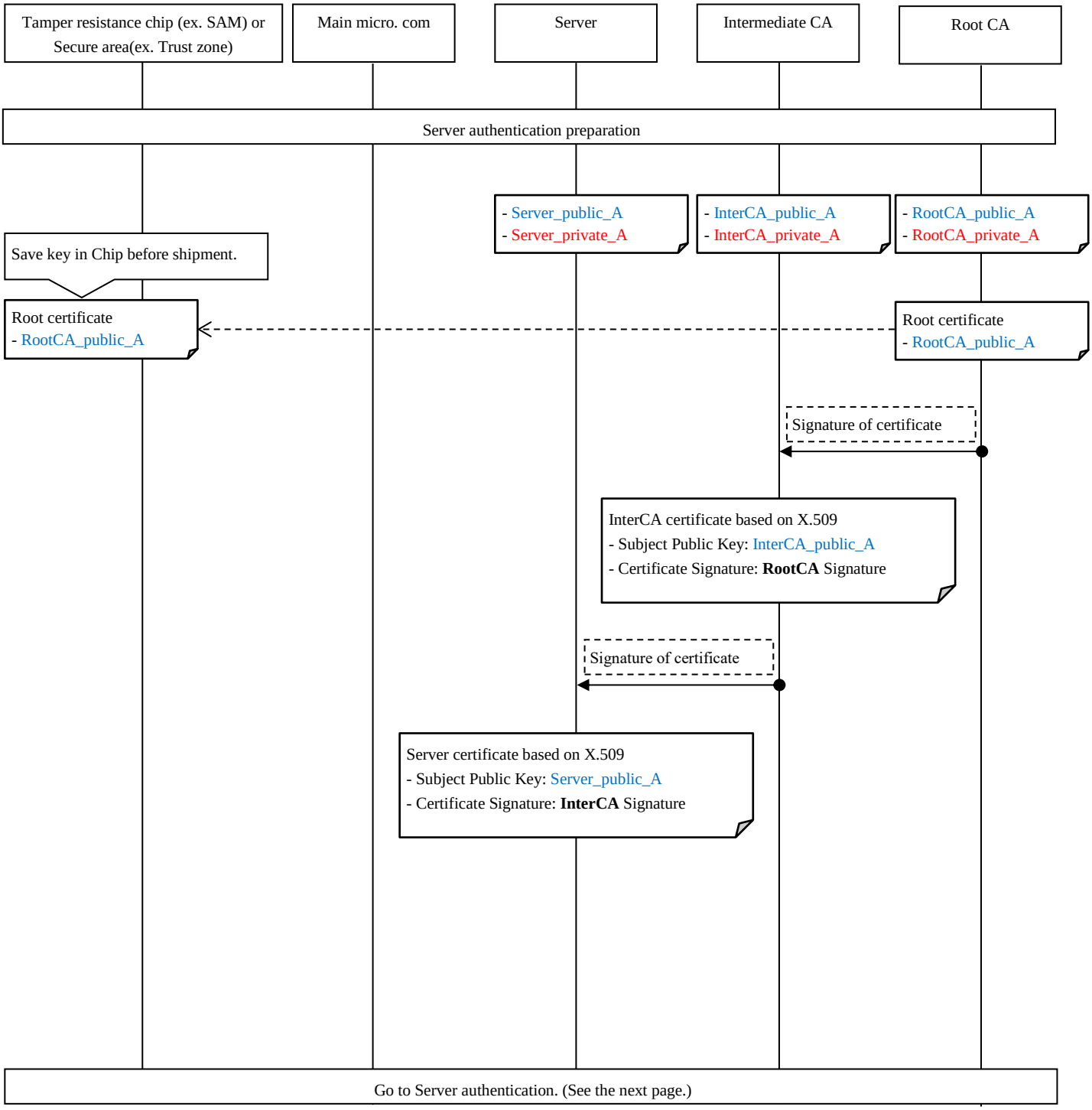



**Fig. 5-1 Server Authentication preparation**

The part of server authentication of server authentication sequence is shown below.

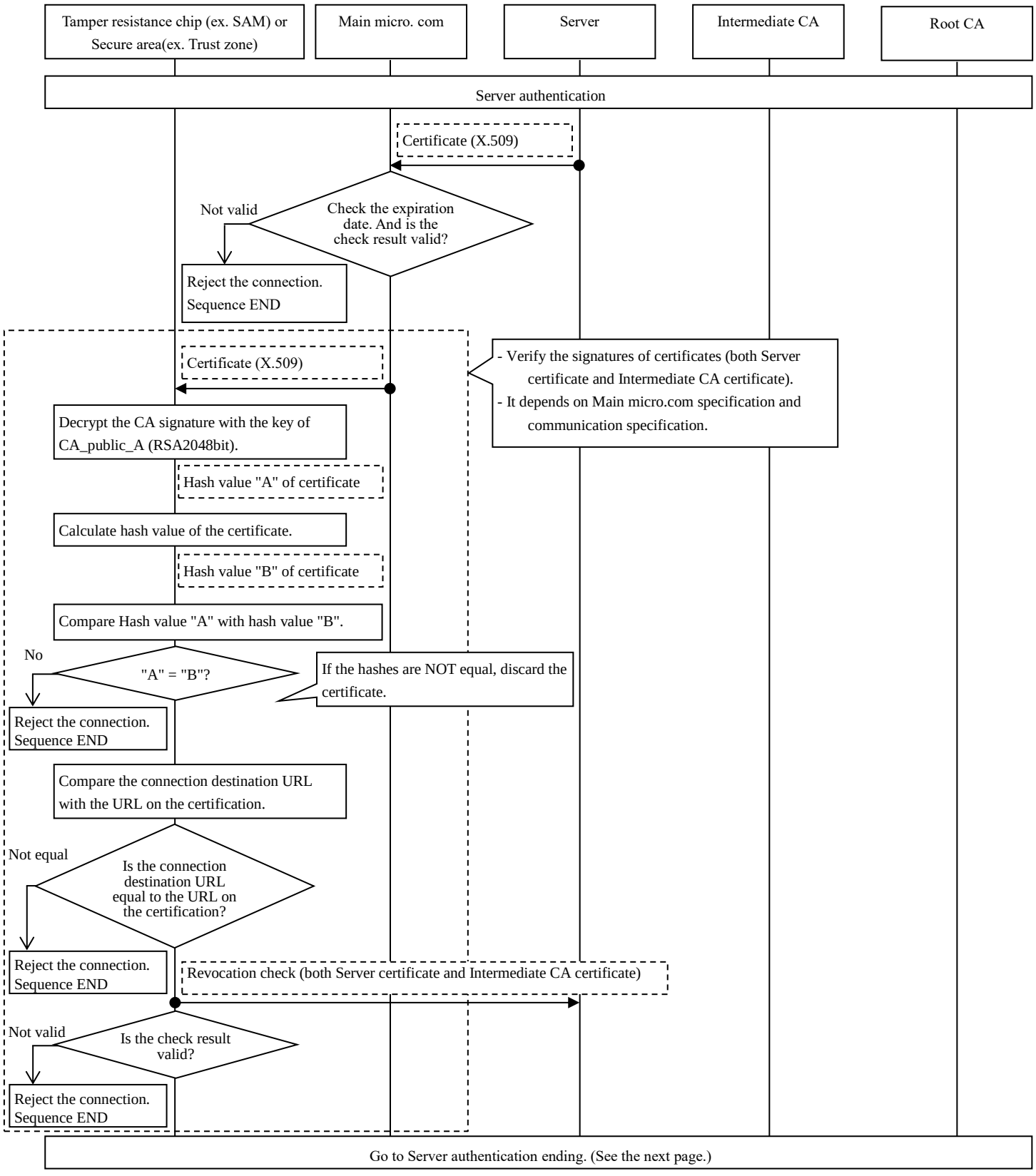



**Fig. 5-2 Server Authentication**

The part of server authentication ending of server authentication sequence is shown below.

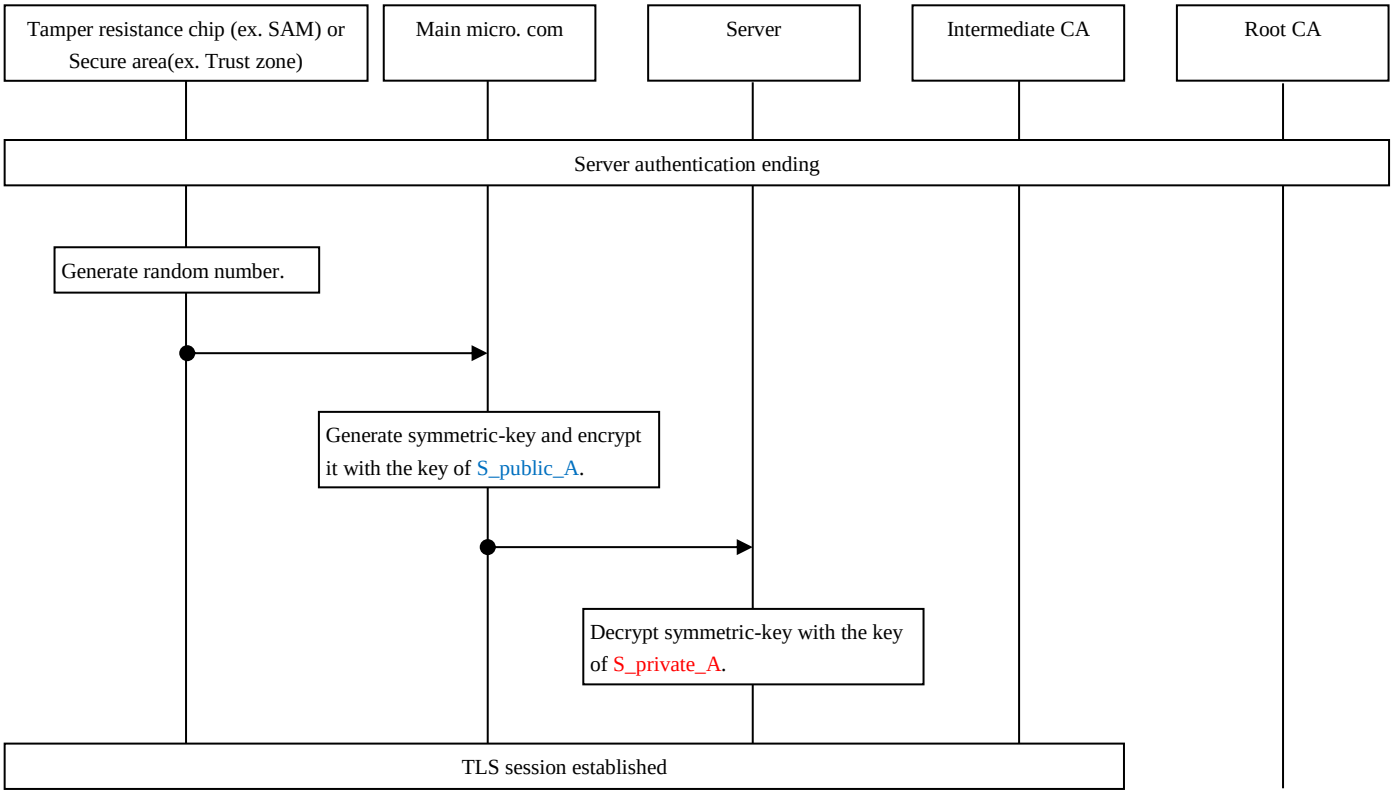



**Fig. 5-3 Server Authentication Ending**

## 5.2. Client Authentication

Client authentication sequence is shown below.

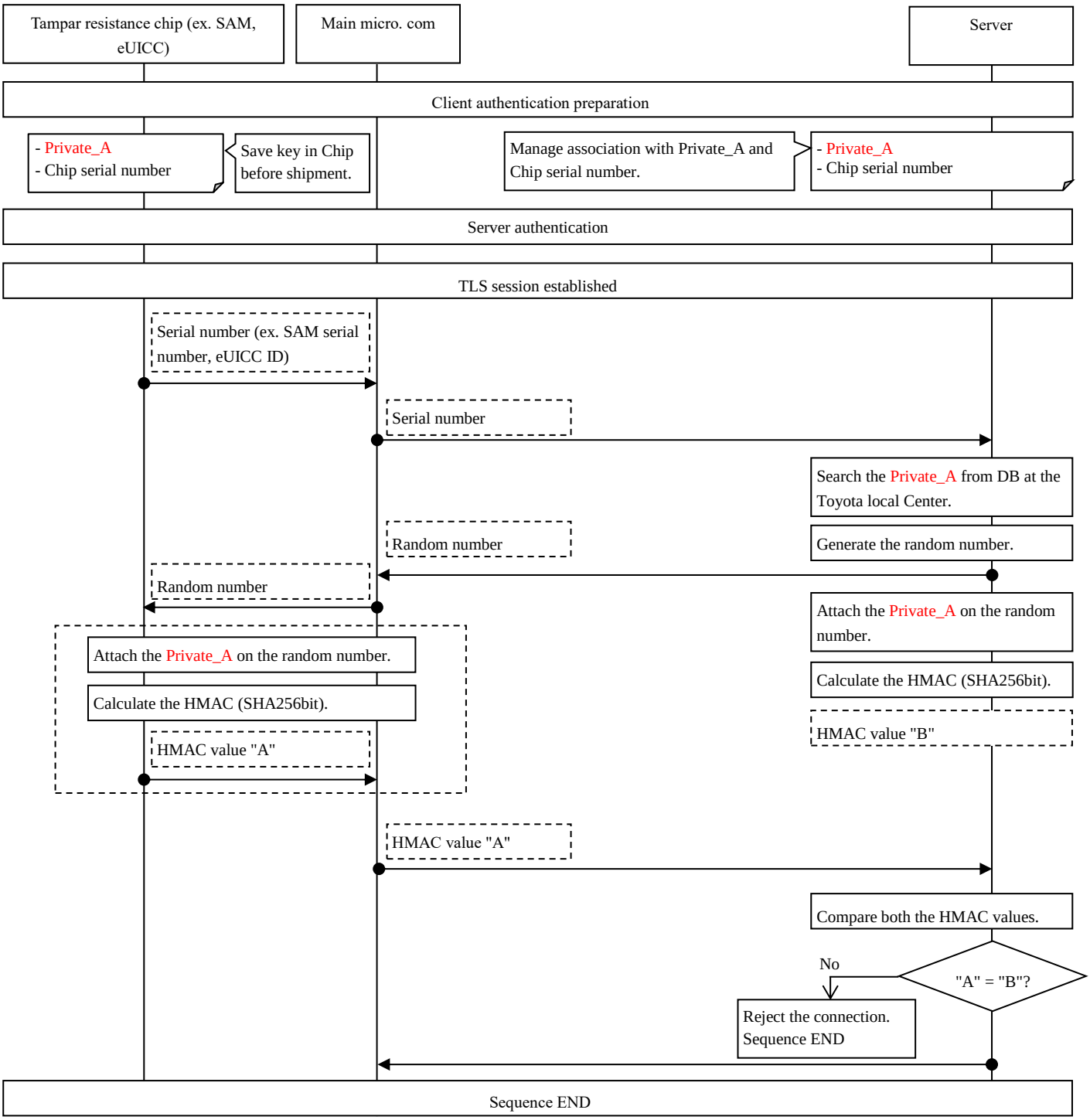



**Fig. 5-4 Client Authentication**