

(11) 特許出願公開番号

特開2017-153101

(P2017-153101A)

(43) 公開日 平成29年8月31日(2017.8.31)

(51) Int.Cl.

F 1

テーマコード (参考)

HO4W 12/06 (2009.01)

HO 4W 12/06

5 J 104

HO4W 84/10 (2009.01)

HO 4W 84/10

5 K 0 6 7

HO4W 88/08 (2009.01)

HO 4W 88/08

HO 4 L 9/32 (2006.01)

HO 4 L 9/00

6 7 5 A

G O 6 F 21/50 (2013.01)

HO 4 L 9/00

6 7 5 B

審査請求 有 請求項の数 14 O L (全 69 頁) 最終頁に続く

(21) 出願番号 特願2017-56418 (P2017-56418)

(22) 出願日 平成29年3月22日 (2017. 3. 22)

(62) 分割の表示 特願2015-145557 (P2015-145557)
の分割

原出願日 平成22年3月5日 (2010.3.5)

(31) 優先權主張番号 61/157,833

(32) 優先日 平成21年3月5日 (2009.3.5)

(33) 優先権主張国 米国 (US)

(31) 優先權主張番号 61/222,067

(32) 優先日 平成21年6月30日 (2009. 6. 30)

(33) 優先權主張国 米国 (US)

(31) 優先權主張番号 61/235,793

(32) 優先日 平成21年8月21日 (2009. 8. 21)

(33) 優先權主張国 米国 (US)

(71) 出願人 510030995

インターデジタル パテント ホールディングス インコーポレイテッド
アメリカ合衆国 19809 デラウェア
州 ウィルミントン ベルビュー パーク
ウェイ 200 スuite 300

(74) 代理人 110001243

特許業務法人 谷・阿部特許事務所

(72) 発明者 サディール ビー. パッター

アメリカ合衆国 08054 ニュージャ
ージー州 マウント ローレル アン ド
ライブ 17

[最終頁に続く](#)

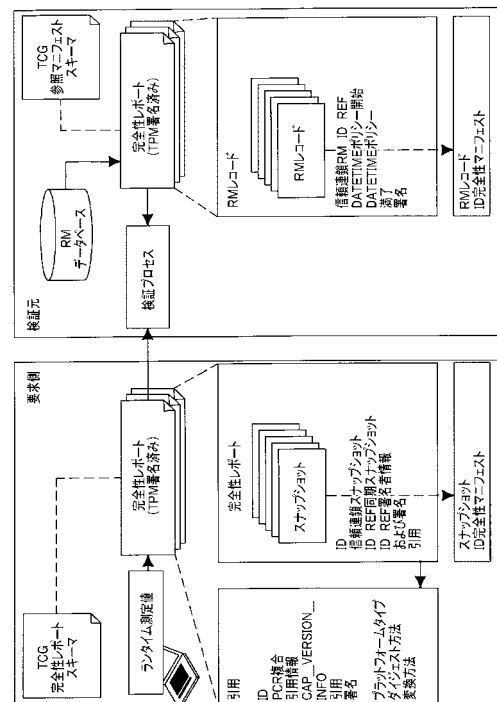
(54) 【発明の名称】 H (e) NB完全性検証および妥当性確認のための方法および機器

(57) 【要約】 (修正有)

【課題】 自律的妥当性確認および半自律的妥当性確認を用いる、H (e) NB (home evolved Node B) の完全性の妥当性確認を可能にする。

【解決手段】 H (e) NBにおいて、H (e) NBのコンポーネントについて完全性メトリックを測定し、H (e) NB上の安全なローカルストレージから信頼できる参照値 (TRV) を取り出し、測定された完全性メトリックをTRVと比較して、コンポーネントの完全性検証チェックの結果を判定し、コンポーネントの完全性検証チェックの結果をプラットフォーム妥当性確認エンティティ (PVE) に報告する。PVE及びH (e) NBはネットワーク上の別個のエンティティである。

【選択図】 図5



【特許請求の範囲】**【請求項 1】**

通信ネットワークに接続されたデバイスの完全性検証を実行する方法であって、前記デバイスにおいて実行される以下のステップ、

前記デバイスにおいて、ソフトウェアコンポーネントと、前記コンポーネントに関連する重大度情報および信頼できる参照値（TRV）を含む関連付けられた属性とのリストを含むデバイス構成データシートを検索するステップと、

前記デバイスにおいて、前記デバイスの前記コンポーネントの少なくとも 1 つに対する完全性メトリックを測定するステップと、

前記デバイスにおいて、前記測定された完全性メトリックを、前記デバイス構成データシートから取得された前記少なくとも 1 つのコンポーネントの TRV と比較して、前記少なくとも 1 つのコンポーネントの完全性検証チェックの結果を判定するステップと、

前記完全性検証チェックが失敗した場合、前記デバイス構成データシートの重大度情報により示されるアクションを実行するステップと

を備えたことを特徴とする方法。

【請求項 2】

前記デバイス構成データシートは、前記デバイス上のローカルストレージに記憶されることを特徴とする請求項 1 に記載の方法。

【請求項 3】

前記デバイス構成データシートは、前記デバイスにおける安全なメモリに記憶されることを特徴とする請求項 1 に記載の方法。

【請求項 4】

前記アクションは、非常信号を送信していることを特徴とする請求項 1 に記載の方法。

【請求項 5】

前記アクションは、前記デバイスを停止していることを特徴とする請求項 1 に記載の方法。

【請求項 6】

前記アクションは、前記デバイスを停止し、およびフォールバックコードの実行を開始していることを特徴とする請求項 1 に記載の方法。

【請求項 7】

前記アクションは、前記少なくとも 1 つの測定されたコンポーネントを隔離していることを特徴とする請求項 1 に記載の方法。

【請求項 8】

前記アクションは、前記デバイスのアクセスまたは機能性を制限していることを特徴とする請求項 1 に記載の方法。

【請求項 9】

前記アクションは、コード修復を開始していることを特徴とする請求項 1 に記載の方法。

【請求項 10】

前記アクションは、完全性検証チェックを失敗した前記少なくとも 1 つのコンポーネントに関連する少なくとも 1 つの失敗した機能性を報告していることを特徴とする請求項 1 に記載の方法。

【請求項 11】

前記デバイス構成データシートは、XML 文書であることを特徴とする請求項 1 に記載の方法。

【請求項 12】

前記デバイス構成データシートは、デジタル署名で署名されることを特徴とする請求項 1 に記載の方法。

【請求項 13】

前記デジタル署名は、前記デバイス構成データシートの前記完全性を判定するために使

10

20

30

40

50

用されることを特徴とする請求項 1 2 に記載の方法。

【請求項 1 4】

更新されたデバイス構成データシートは、コード修復が提供されることを特徴とする請求項 1 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本出願は通信に関する。

【背景技術】

【0002】

関連出願の相互参照

本出願は、あたかも本明細書に完全に記載されているかのように、すべてが参照によって組み込まれている、2009年3月5日出願した米国特許仮出願第61/157,833号明細書、2009年6月30日出願した米国特許仮出願第61/222,067号明細書、2009年8月21日出願した米国特許仮出願第61/235,793号明細書、および2009年9月3日出願した米国特許仮出願第61/239,698号明細書の利益を主張する。本出願は、あたかも本明細書に完全に記載されているかのように、参照によって組み込まれている、同時に提出した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に関連する。

【0003】

フェムトセルとしても知られているH(e)NB(home evolved Node B)は、概して、ホスティング側(HP)と呼ばれる関係者の構内または宅内に置かれる3Gネットワークへの小型の可搬型アクセスポイントである。H(e)NBは、小さい、指定された地理的エリア内の移動通信およびサービスのための仲介となる。H(e)NBは、構内または工場環境など、従来は(不良無線条件のせいで)アクセス不可能だったエリア内でモバイルサービスを提供するのに使われ得る。H(e)NBはブロードバンドインターネットおよびモバイルネットワークへの統一アクセスポイントになり得るので、H(e)NBは、SOHO(small office home office)セクタ用の選択肢でもある。

【0004】

本出願は、具体的なセキュリティ要件を提起し得る。例えば、こうしたデバイスは、i) モバイルハンドセットが従来見なされていたような、極秘データの格納および取扱いのための閉じた、不変の環境とはもはや見なされず、ii) こうした特殊デバイスは一般に、H(e)NBの主たる関係者として、H(e)NBを操作して移動通信端末のユーザにサービスを提供するモバイルネットワークオペレータ(MNO)の直接の物理的制御下ではなく、iii) こうしたデバイスは概して、安全でないリンクを介して、また、継続的であるよりもむしろ断続的であり得るようにコアネットワークに接続される。

【0005】

モバイル通信ネットワークの既存または標準化された技術は、ネットワークが、それが操作するH(e)NBが、H(e)NBが従来の認証ステップを通った場合でさえも、信用できるものになると十分に見なすための方法を提供することができない。したがって、必要とされるものは、MNOがデバイスの信用性、すなわち、完全性を認証(authenticate)し、且つ妥当性確認(validate)し、このようなデバイスを管理しプロビジョニングするのを助ける方法である。

【発明の概要】

【0006】

自律的妥当性確認および半自律的妥当性確認を用いる、H(e)NB(home evolved node-B)完全性の妥当性確認を可能にする機器および方法を本明細書で開示する。

【図面の簡単な説明】

【0007】

添付の図面とともに、例として挙げられる以下の説明により、より詳細に理解すること

10

20

30

40

50

ができよう。

【図 1】モジュール、機能性およびコンポーネントの編成例を示す図である。

【図 2】コンポーネントおよび機能性の編成例を示す図である。

【図 3】ソフトウェアダウンロード用プロビジョニングのための T R O 6 9 アーキテクチャ例を示す図である。

【図 4】基本的な完全性測定および報告の例を示す図である。

【図 5】完全性レポートおよび参考資料の例を示す図である。

【図 6】妥当性確認レポートと参照マニフェストとの比較の例を示す図である。

【図 7】参照マニフェスト中のコンポーネント情報の例を示す図である。

【図 8】証明書管理アーキテクチャの例を示す図である。

10

【図 9】H (e) N B (home evolved-Node B) (H (e) M S) の再構成の例を示す図である。

【図 10】自律的妥当性確認 (A u V) 修復の例を示す図である。

【図 11】ファイルパッケージ形式の例を示す図である。

【図 12】半自律的妥当性確認 (S A V) のネットワークアーキテクチャ例を示す図である。

【図 13 A】S A V プロシージャのためのフローチャート例を示す図である。

【図 13 B】S A V プロシージャのためのフローチャート例を示す図である。

【図 14】S A V 修復のためのフローチャート例を示す図である。

【図 15】完全性チェックの結果例を示す図である。

20

【図 16】失敗した機能性のリスト例を示す図である。

【図 17 A】プラットフォーム妥当性確認および管理 (P V M) のためのエンティティセットおよびその関係並びにインタフェースの例を示すブロック図である。

【図 17 B】P V M のためのエンティティセットおよびその関係並びにインタフェースの別の例を示すブロック図である。

【図 18 A】プラットフォーム妥当性確認エンティティを用いる妥当性確認の方法例を示す信号図である。

【図 18 B】プラットフォーム妥当性確認エンティティを用いる妥当性確認の方法例を示す信号図である。

【図 18 C】プラットフォーム妥当性確認エンティティを用いる妥当性確認の方法例を示す信号図である。

30

【図 19】L T E ワイヤレス通信システム／アクセスネットワークを示す図である。

【図 20】L T E ワイヤレス通信システムを示す例示的なブロック図である。

【発明を実施するための形態】

【0008】

これ以降において言及する場合、「W T R U (ワイヤレス送受信ユニット)」という用語は、U E (ユーザ機器)、移動局、固定もしくは移動加入者ユニット、ページャ、セルラー電話、P D A (携帯情報端末)、コンピュータ、またはワイヤレス環境において動作することが可能な他のどのタイプのデバイスも含むが、それに限定されない。これ以降において言及する場合、「基地局 (b a s e s t a t i o n) 」という用語は、ノード B、サイトコントローラ、アクセスポイント (A P)、ゲートウェイ、C P E (顧客構内機器)、またはワイヤレスもしくはワイヤライン環境において動作することが可能な他のどのタイプのインタフェースデバイスも含むが、それに限定されない。これ以降で言及する場合、「H M S」という用語は、H M S (H o m e N o d e B M a n a g e m e n t S y s t e m)、H e M S (H o m e E n h a n c e d - N o d e B M a n a g e m e n t S y s t e m) を含むが、それに限定されず、この 2 つはまとめて、H (e) M S、デバイス管理システム (D M S)、構成サーバ (C S)、自動構成サーバ (A C S)、または「基地局」の構成もしくは機能性を管理する他の任意のタイプのシステムと呼ぶこともできる。「W T R U」および「基地局」という用語は、相互排他的ではない。例えば、W T R U は、H (e) N B (e n h a n c e d H o m e N o d e - B) であり

40

50

得る。これ以降で言及する場合、「情報理論的に安全 (information-theoretically secure)」という用語は、完全に安全、無条件に安全、および情報理論的にほぼ安全を含むが、それに限定されない。これ以降で言及する場合、「信頼 (trust)」、「信頼できる (trusted)」、および「信用できる (trustworthy)」という用語、並びにその変化形は、ユニットがある特定の方式で機能するかどうかを評価する、数量化可能であり観察可能な方式を示す。

【0009】

自律的妥当性確認 (AuV) および半自律的妥当性確認 (SAV) を用いて、H (e) NB (home evolved node-B) 完全性検証 (integrity verification) および妥当性確認を行う機器および方法について本明細書に記載する。AuV および SAV に共通の詳細を記載し、続いて AuV および SAV に関して実装の詳細を記載する。

10

【0010】

妥当性確認方法において使われる信頼できる参照値 (TRV) を判定する方法について本明細書に記載する。デバイス完全性検査は、妥当性確認方法に共通のプロシージャである。デバイス完全性検査用に、コンポーネントについてされた測定の完全性をチェックできるように、1組の TRV が必要とされる。コンポーネントのこのような完全性検査は、コンポーネントがロードされる前に行われるべきであることが望まれ得る。このような TRV は、使われる前にそれ自体によって認証され完全性を確実にされ得ることも望まれ得る。

20

【0011】

完全性チェックを実施し、TRV を提供し生成するために、異なる完全性チェック方法を用いることができる。例えば、コードに対応する TRV を生成する方法は、デジタル署名方法を含んでよく、ハッシュベースのメッセージ認証コードまたは暗号化ベースのメッセージ認証コードも検討してよい。

【0012】

デジタル署名方法について本明細書に記載する。デジタル署名方法では、公開鍵暗号技術を用いることができる。H (e) NB は、その私有鍵 (private key) を使ってチェック語を暗号化することによって、モジュールのハッシュ (または、概してチェック語) にデジタル署名することができる。暗号化されたチェック語は次いで、プラットフォーム妥当性確認エンティティ (PVE) に送られればよく、PVE において H (e) NB の公開鍵で復号し、TRV と比較することができる。ローカル完全性チェックのために、参照完全性チェックは、製造元によって署名され、H (e) NB 内部でローカルに検証され得る。非限定的例として、テーブル 1 は、幾つかのデジタル署名方法を明らかにする。

30

【0013】

【表 1】

名称	タイプ	特性	最小鍵サイズ
デジタル署名標準	FIPS186-2デジタル署名	SHA-1ハッシュに基づくデジタル署名。特許なし、ライセンスなし。米連邦政府の輸出規制が該当する	1024ビット
RSAデジタル署名	RSAデジタル署名 (FIPS認可済み)	以前特許化済み(2000年に失効)	1024ビット
楕円曲線デジタル署名	楕円曲線デジタル署名	楕円曲線鍵技術に基づく技術	160ビット

テーブル1

【0014】

ハッシュアルゴリズムおよびハッシュベースのメッセージ認証コードについて本明細書に記載する。ハッシングは、その入力の一意（またはほぼ一意）および非可逆（またはほぼ非可逆）の要約を生じる単方向またはほぼ一方向の関数である。多くのケースにおけるデジタル署名は、暗号化されたハッシュに過ぎない。デジタル署名方法は、公開／私有鍵ペアを使うことができ、MAC（メッセージ認証コード）は、共有秘密鍵を使うことができる。チェック語は、組み込まれた秘密鍵（secret key）を有するモジュール（連結されたモジュールおよび鍵）を介して作成することができる。非限定的例として、テーブル2は、幾つかのハッシュアルゴリズム並びにハッシュベースのメッセージ認証コード方法を明らかにする。

【0015】

【表 2】

名称	タイプ	特性	最小鍵サイズ
SHA-1, SHA-256, SHA-512	ハッシュアルゴリズム	FIPS認可済み	160, 256, 512ビット
普遍的メッセージ認証コード	ハッシュベースのMAC	最速ハッシュベースのアルゴリズム	32, 64, 96ビット
RACE完全性プリミティブ評価メッセージダイジェスト-160	ハッシュアルゴリズム	欧州におけるECのR&D	160ビット
TIGER(2)	ハッシュアルゴリズム	64ビットプラットフォーム上での効率的動作のために設計された	192ビット
HMAC-SHA1-96	ハッシュベースのMAC	ハッシュ用にSHA-1を使う	96ビット
WHIRLPOOL	ハッシュベースのMAC	特許化されていない	512ビット

テーブル2

【0016】

暗号化ベースのメッセージ認証コードについて本明細書に記載する。チェック語は、ハッシュアルゴリズムによって作成し、次いで、秘密鍵を使って暗号化することができる。非限定的例として、テーブル3は、幾つかの暗号化ベースのメッセージ認証コード方法を

明らかにする。

【0017】

【表3】

名称	タイプ	特性	最小鍵サイズ
DES-CBC-MAC	暗号MAC	DESベース	64ビット
CMAC	暗号MAC	対称鍵ブロック暗号アルゴリズムを使う暗号化ベースのMAC	64, 128, 192, 256
CCM	暗号MAC	カウンタモード暗号化とともに暗号ブロック連鎖を使う	128, 192, 256

テーブル3

10

【0018】

完全性メトリックは、ソフトウェアコンポーネントに対する完全性方法の実行によって生成されたダイジェスト（例えば、暗号ハッシュ値）である。コンポーネントは、本明細書において、完全性検査の最も小さい可能単位と見なされる。個々のバイナリ実行可能または事前実行可能ファイルが、コンポーネントの例である。一方、モジュールは、本明細書において、ソフトウェアパッケージの製造元が、証明し、配布するための最も小さい単位と見なされる。本説明の残りでは、概して、図1に示すように、1) コンポーネントは、常に1つまたは複数のモジュールからなることができ、2) どの1つのモジュールも、コンポーネント中に一度だけ現れる（すなわち、1つのモジュールが、2つのコンポーネント中に現れることはできない）と見なす。AuVおよびSAVでのデバイス完全性チェックおよび妥当性確認をサポートするために、モジュール、重大度に対応する参照完全性メトリック（RIM）など、ソフトウェアモジュールおよびそれに関連付けられた属性のリスト、並びに他の情報が提供されなければならない場合もある。参照完全性メトリック（RIM）は、個々のモジュールの完全性に対する参照値として働く。AuVのケースでは、リストは、製造元によって生成し、デバイスに安全に格納することができ、SAVのケースでは、リストは、製造元によって生成し、プラットフォーム妥当性確認エンティティ（PVE）（全モジュール）に与え、また、H(e)NBにプロビジョニングすることができる（多段階スタートアップ実装における段階1および段階2モジュール用）。どのようにソフトウェアモジュールが編成され、構造化され、または格納されるか、並びにこのようなモジュールのどのような種類がデバイスに存在し得るかは、H(e)NB実装形態に依存してよく、共通仕様言語を使って、モジュールおよびその属性を指定することができる。

20

30

【0019】

例えば、XML（拡張マークアップ言語）およびASN.1（抽象構文記法1）ベースの方法が、共通仕様言語の実装に用いられ得る。デバイス構成データシートは、ソフトウェアモジュールおよびモジュールに関連付けられた様々な属性のリストを含む。データシートは、コンポーネントおよび機能性へのモジュールの分類も指定し得る。

40

【0020】

H(e)NBのコンポーネントおよび／またはモジュール並びに関連付けられた属性を指定するための共通の高移植性言語を提供することができるソフトウェアモジュール属性のXMLベースの仕様について本明細書に記載する。可搬的に、およびH(e)NBアーキテクチャ不問なやり方で情報を提供するために、モジュールを指定する言語が進化されなければならない。言語は、XMLスキーマおよびXML文書を含むXML言語と同様でよい。モジュールの形式および様々な属性は標準化することができ、すべての製造元が、ソフトウェアモジュールを規定の形式で記述するデバイス構成データシートを提供する。形式は、XMLスキーマと同様でよく、デバイス構成データシートはXML文書と同様で

50

よい。XML署名は、完全性、メッセージ認証および／または署名者認証を行うための、デジタル署名を追加するというサポートを提供する。バイナリXMLとは、より簡潔な表現であり、解析コストを削減し、且つあるエンティティから別のエンティティへの構成データの通信用の必要帯域幅を削減するための基礎として使うこともできる。XMLスキーマの例は、テーブル4に示してあり、製造元がそのモジュールを指定することができる標準形式でよい。

【0021】

【表4】

XMLスキーマ	10
<pre> <?xml version="1.0"?> <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"> <xs:element name="Manufacturer Identification"> <xs:complexType> <xs:sequence> <xs:element name="Name" type="xs:string"/> <xs:element name="URL" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element> <xs:element name="Module Name"> <xs:complexType> <xs:sequence> <xs:element name="Version" type="xs:string"/> <xs:element name="Stage" type="xs:string"/> <xs:element name="Severity" type="xs:string"/> <xs:element name="Author" type="xs:string"/> <xs:element name="Dependency" type="xs:string"/> <xs:element name="Integrity Algorithm" type="xs:string"/> <xs:element name="Reference Integrity Metric" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>+ <Signature ID?> <SignedInfo> <CanonicalizationMethod/> <SignatureMethod/> (<Reference URI? > (<Transforms>)? <DigestMethod> <DigestValue> </Reference>)+ </SignedInfo> <SignatureValue> (<KeyInfo>)? (<Object ID?>)* </Signature> </xs:schema> </pre>	20 30 40
「?」はゼロまたは一度の出現を示し、「+」は一度または複数の出現を示し、「*」はゼロ以上の出現を示す	

テーブル4

【0022】

製造元は、デバイス構成データシートを提供し、デジタル署名でシートに署名することができる。このデバイス構成データシートは、A u V用のH (e) N Bの所で維持することができる。チェックが失敗したケースでは、デバイス構成シート自体のデジタル署名が検証された場合、適切なアクションをとることができる。というのは、このことは、任意の失敗モジュールの影響についての情報を含む、ソフトウェアの属性が、ソフトウェアモジュール自体（すなわち、バイナリイメージ）が変化しており完全性検査に失敗していても、損なわれていないことを意味するからである。S A Vのケースでは、デバイス構成シートは、デバイスおよびP V Eの所で維持することができる。本明細書に記載するように、S A Vをサポートするための追加アクションを追加することもできる。

10

【0023】

H (e) N Bのコンポーネントおよび関連付けられた属性を指定するための共通の高移植性言語を提供することができる、ソフトウェアモジュール属性のA S N . 1ベースの仕様について本明細書に記載する。遠隔通信およびコンピュータネットワーク接続において、A S N . 1は、データを表し、符号化し、伝送し、デコードするデータ構造を記述する、標準的であり柔軟な表記法である。A S N . 1は、マシン固有符号化技法に依存しないオブジェクトの構造を記述するとともに、曖昧さをなくす精密な公式表記法である公式規則セットを提供し得る。通信プロトコル用のメッセージを定義するのに一般に使われるように、A S N . 1は、それに関連付けられた符号化規則とともに、バイナリ符号化を結果的にもたらす。インターネットプロトコルであるH T T PおよびS M T Pなど、他の通信プロトコルは、テキストタグおよび値を使って、時にはA B N F（拡張バックスナウア記法）表記法に基づいて、メッセージを定義する。この定義は、符号化も定義するが、テキスト形式である。

20

【0024】

A S N . 1手法は、より効率的であると信じられており、圧縮符号化規則を用いて、確かにより簡潔な符号化を提供する。テキスト手法は、（テキスト列の作成および解析により）実装するのがより簡単であり、符号化されたメッセージを読むだけでよいので、デバッグするのがより簡単であると主張されている。M e g a c oプロトコルのケースでは、A S N . 1およびA B N Fに基づいて2つの符号化が定義された。

【0025】

A S N . 1 X M L符号化規則（X E R）は、A S N . 1表記法を使って定義されたデータ構造のテキスト符号化を可能にする。ユーザとの間でデータを提示し入力するという唯一の目的のために、一般的文字列符号化規則も定義された。デバイス完全性メトリックを伝達するA S N . 1の例を、テーブル5に示すことができる。

30

【0026】

【表 5】

ASN.1	
DeviceIntegrityMeasurementsType DEFINITIONS ::= BEGIN	
ManufacturerIdentification ::= {	
Name	IA5String,
URL	IA5String
}	
Modules ::= SEQUENCE {	
Version	INTEGER,
Stage	INTEGER,
Severity	INTEGER,
Author	IA5String,
Dependency	IA5String,
IntegrityAlgo	IA5String,
RIM	IA5String
}	
DigitalSignature ::= {	
SignedInfo	SignedInfoType,
KeyInfo	KeyInfoType,
SignatureValue	IA5String
}	
END	
タイプ SignedInfoType および KeyInfoType は、DeviceIntegrityMeasurements Type と同様に定義され得る	

テーブル 5

【0027】

デバイスにある各ソフトウェアモジュールにとって、それと関連付けられたモジュール属性がネットワークに知られている場合、SAVプロシージャ中に、H(e)NBは、ローカル完全性チェックプロシージャ中の完全性チェックに失敗した全モジュールの識別(ID)のリストだけをPVEに送ればよい。ネットワークは、PVEを経由して、特定のソフトウェアモジュールの関連属性およびモジュールの失敗の影響を知ることになる。この情報は、本明細書に記載するように、ネットワークがとる次のステップの評価を行うのに用いることができる。

【0028】

H(e)NBに送信されると見なすことができ、H(e)NB管理システム(H(e)MS)など、信頼できるサードパーティ(TTP)から、デジタル証明書(digital certificate)または署名されたメッセージとしてプロビジョニングすることができるソフトウェアモジュール属性について本明細書に記載する。例えば、コードイメージに対する全体的情報要素は、H(e)NBの製造元およびモジュールコードイメージのダイジェストまたはRIMを生成するのに用いられ得る完全性方法を含み得るが、それに限定されない。

【0029】

コンポーネント特有の情報を記述するための方法について本明細書に記載する。1つまたは複数のコンポーネントが、ソフトウェアモジュールを成す。コンポーネントとは、完全性検査の基本的単位である。各コンポーネントに関連付けられた、1つの信頼できる参照値(TRV)がある。コンポーネント特有の情報要素は、コンポーネント説明に対応する、一意に識別可能なIDであるコンポーネントIDを含み得る。これは、1つのTRVでチェックされるべきコードの単位のIDである。情報要素は、H(e)NB上での完全性検査機構が、コンポーネントの測定値を比較して、コンポーネントの完全性を検証するのに使うことができるTRVをさらに含み得る。

【0030】

モジュール特有の情報要素は、H(e)NB内部の特有のモジュール機能を記述するモジュール説明およびモジュールを製造元に対して一意に識別するモジュールIDを含み得るが、それに限定されない。この情報要素は、このモジュールがマップされる先のH(e)

）NBの特有の機能性を識別する機能説明およびグローバルに識別可能なIDでよく、複数のベンダに渡って標準化され、機能説明に対応し得る機能IDも含み得る。この情報要素は、このモジュールがマップする先のコンポーネントを識別するコンポーネントIDおよびモジュールのバージョン番号を示すリリースバージョンをさらに含み得る。コンポーネントとモジュールとの間に1対1のマッピングがあるケースでは、モジュール特有の情報は事実上、コンポーネント特有の情報と同一であり得る。

【0031】

モジュール特有の情報要素は、システムの機能性に関する、現在のソフトウェアの完全性チェックの失敗の影響を指定する重大度分類も含み得る。例えば、複数レベル重大度分類システムが存在し得る。例えば、重大度1は、H(e)NB機能性に対して高い影響を結果的に生じるモジュール／機能の失敗でよく、システムの停止動作を保証し得る。モジュール／機能の失敗は、フォールバックコードイメージ(FBC)に基づいて、システムに沿った乱れを結果として生じ得る。この場合、ネットワークベースのデバイス管理システム(デバイスがH(e)NBである場合はH(e)MSとなる)との通信が可能であり得る。FBCは、指定されたH(e)MSに非常信号を送ることが可能であり得る。さらに、ネットワークが開始したファームウェア／ソフトウェアアップデートをサポートすることもできる。例えば、H(e)NBの信頼できる環境(TrE)のためのどのモジュールまたはコンポーネントも、重大度1をもち得る。重大度2は、制限されたH(e)NB機能性を結果的に生じることがあるモジュール／機能の失敗でよく、この失敗は、フルH(e)NB機能性のサブセットとして部分的に機能することができ、またはフルH(e)NB機能性のサブセットをサポートすることができる。この場合、セキュリティゲートウェイ(SeGW)との通信が可能であり得る。重大度3は、システムのコア機能性に影響し得ないモジュール／機能の失敗でよいが、依然として、失敗のケースでは早期修復を求めるのに十分な程重要と見なされ得る。失敗したモジュール／機能は、即座のファームウェア／ソフトウェアアップデートプロシーダを介して置き換え、後続リブートにより妥当性確認することができる。重大度4は、システムのコア機能性に影響し得ないモジュールの失敗でよい。失敗したモジュール(複数可)は、通常ファームウェア／ソフトウェアアップデートスケジュールを介して置き換えることができる。

【0032】

妥当性確認方法のための報告プロシーダまたは方法について本明細書に記載する。AuV用に、デバイス完全性チェックの全プロシーダを、ローカルに実施することができる。完全性チェックが失敗した場合、非常信号をH(e)MSに送って、失敗を示すことができる。後続アクションは、送付担当者から、課題を解決し、またはデバイスを検疫(quarantine)するために広がり得る。修復は、失敗したモジュールのリストが修復サーバ／H(e)MSに報告され得るケースにおいて実施することができる。SAVのケースでは、完全性チェックに失敗した機能性のリストが、PVEに報告され得る。

【0033】

モジュールは、製造元の実装に依存する。コンパイルされた1組のソフトウェアモジュールは、オブジェクトイメージを形成し得る。完全性チェックは、オブジェクトイメージチャンクに対して実施することができる。したがって、完全性チェックがそれに対して行われる1組のモジュールを組み合わせたコンポーネントが導入されている。1つのモジュールは、コンポーネント中で一度現れ、ただ1つのコンポーネント中で現れる(すなわち、1つのモジュールが、2つのコンポーネント中で現れることはできない)。このように、完全性チェックが実施されると、モジュールは一度だけ調べられる。H(e)NBの製造元(個々のどのソフトウェアモジュールの製造元と同一でも、異なってもよい)は、アーキテクチャに基づいて、デバイス完全性チェックのために、モジュールをコンポーネントにどのようにして区分するかを決定する。

【0034】

機能性は、H(e)NBの要件および機能アーキテクチャに基づいてよく、標準化された識別子でよい。例えば、Iuインタフェースおよび移動管理は、機能である。モジュール

ルは、この２つの機能の間で共有することができる。したがって、コンポーネント（完全性チェック単位である）が完全性チェックに失敗すると、影響を受けたモジュールが分かる。各モジュールは、それに関連付けられた機能性をもつので、失敗した機能性のリストが導出され得る。この失敗した機能性のリストは、SAVにおいてPVEに送られる。

【００３５】

機能性IDについて本明細書に記載する。アーキテクチャの実装は、ソフトウェアモジュールの数およびタイプを支配する。複数の製造品および／または関係者（モバイルネットワークオペレータなど）に渡って報告構造および手順を調和させるために、報告は、実際のモジュールではなく機能性に基づいて行うことができる。ソフトウェアモジュールは、その機能性に基づいてグループ化することができる。機能性IDは、機能性説明に基づいてモジュールを分類するための手段を提供する。テーブル６は、現在知られているものに基づいて導出されている機能性の一部を列挙している。このリストは、拡張し標準化することができる。テーブル６中で、最終有効桁が１～９の番号は、将来の使用または拡張性のために取り置かれている。

【００３６】

【表６】

機能性ID	機能性説明
10	H(e)MSサブシステムセキュアブートローダ
20	UuインタフェースTrE
30	Iuhインタフェース完全性の妥当性確認エンジン
40	HGmインタフェースフォールバックコード
50	HUtインタフェースオペレーティングシステム
60	S1-MMEインタフェースH(e)MSサブシステム
70	S1-UUuインタフェース

【００３７】

10

20

80	I2(SIP) Iuhインタフェース
90	Iu-CSインタフェースHGMインタフェース
100	Iu-PSインタフェースHUtインタフェース
110	E、Nc、NbSI-MMEインタフェース
120	RUAサービスSI-Uインタフェース
130	HNBAPサービスI2(SIP)インタフェース
140	HNB GW発見Iu-CSインタフェース
150	HNB登録Iu-PSインタフェース
160	HNB E、Nc、Nbインタフェース用のWTRU登録
170	アクセス制御管理RUAサービス
180	時間管理HNBAPサービス
190	CSG管理HNB GW発見
200	移動性管理HNB登録
210	HNB用のNASノード選択機能UE登録
220	ページング最適化アクセス制御管理
230	トランスポートアドレスマッピング時間管理
240	請求CSG管理
250	緊急サービス移動性管理
260	QoS管理NASノード選択機能
270	ローカルIPアクセスページング最適化
280	管理リモートアクセストランスポートアドレスマッピング
290	旧来のCN請求のHNBサポート

10

20

【 0 0 3 8 】

300	着信ハンドオーバーサポート緊急サービス
310	ローミングQoS管理
320	MSC SGSNローカルIPアクセスへのSCCP無接続通信
330	OAMサブシステム管理リモートアクセス
340	旧来のCN用の表示サブシステムHNBサポート
350	USIMサブシステム着信ハンドオーバーサポート
360	HPMサブシステムローミング
370	MSC SGSNへのIMS相互作用SCCP無接続通信
380	IP-PABXインタフェースOAMサブシステム
390	セキュリティ機能表示サブシステム
400	RAB管理USIMサブシステム
410	無線資源管理HPMサブシステム
420	Iuリンク管理IMS相互作用
430	Iu Uプレーン(RNL)管理IP-PABXインタフェース
440	Iu調整セキュリティ機能
450	プロビジョニング機能RAB管理
460	ハードウェア障害無線資源管理
470	Iuリンク管理
480	Iu Uプレーン(RNL)管理
490	Iu調整機能
500	プロビジョニング機能
510	ハードウェア障害

30

40

テーブル6

50

【0039】

コンポーネントIDについて本明細書に記載する。複数のデバイス完全性チェックを調和させるために、モジュールは、生成されたイメージに基づいて分類することができる。1組のオブジェクトファイルを、イメージファイルの中に一緒にアーカイブすることができる。このようなモジュールグループは、同じコンポーネントIDを含み、まとめて完全性をチェックされ、したがって、1つのコンポーネントに対して信頼できる1つの参照値（TRV）をもつ。各ソフトウェアモジュールは、それ自体の参照完全性メトリック（RIM）を伴うので、コンポーネントの信頼できる参照値（TRV）は、関連付けられたRIMをそれぞれがもち得る、1つまたは複数のソフトウェアモジュールの連結のダイジェスト（例えば、ハッシュ）として取得することができる。1つのコンポーネントIDで現れるモジュールは、別のコンポーネントIDで現れる同じモジュールとは異なる機能性IDにマップされ得ることに留意されたい。このプロセスは、製造元に、そのアーキテクチャおよびコンパイラに基づいて柔軟性を与え、例えば、オブジェクトイメージまたはSAV完全性チェックの段階どちらかに基づいて、モジュールのグループ化を可能にする。

10

【0040】

モジュールIDは、ソフトウェアの様々なモジュールを追跡するのに使われ、標準化することは不可能ではないが、標準化しなくてよい。モジュールIDが標準化されない場合、どのモジュールおよび何個のモジュールが存在するかの決定は、製造元に一任してよい。モジュールIDは、ファームウェア／ソフトウェアアップデートパッケージを提供し、追跡し、組み立てるのに使うことができる。

20

【0041】

モジュール、コンポーネントおよび機能性など、様々な識別子の間の関係を編成し、述べる方法および構造について本明細書に記載する。図1は、一例である方法および構造を示す。ソフトウェアアーキテクチャは、モジュールの数およびタイプを定義する。こうしたモジュールは、その機能性および完全性チェック単位に基づいて分類される。複数のモジュールからなるコンポーネントは、独自のTRVをもつ。任意のコンポーネントの、そのTRVを使う完全性検査が失敗した場合、コンポーネント自体が変えられるか、またはそのダイジェストがTRVの値と同じでなくなっているか、またはコンポーネントに対応するTRVが変えられている。いずれのケースでも、完全性チェックが失敗すると、モジュールと、完全性検査に失敗したコンポーネントとの間のマッピング並びにモジュールと機能性との間のマッピングを用いて、失敗した（または少なくとも「影響を受けた」）機能性のリストを判定することができる。影響を受けた機能性の識別子のリストは、H(e)MSまたはPVEに伝達され得る。

30

【0042】

図2は、コンポーネントおよび機能性の構造例を示す。図に示すように、コンポーネントが、完全性チェックがそれに対して実施される単位であるとき、コンポーネントは、製造元によって決定され得る。各コンポーネントに、機能性のリストを関連付けることができる。コンポーネントは機能性に基づく。したがって、コンポーネントが完全性チェックに失敗すると、失敗した機能性のリストを組み立てることができる。コンポーネントは、そのロード順の順序で、または或いは、実行順の順序で編成することができる。したがって、コンポーネント1がチェックに失敗した場合、コンポーネント1にある機能をローディングまたは実行のどちらかに使うコンポーネント2の機能性も失敗する可能性がある。

40

【0043】

失敗した完全性チェックに基づいて、失敗した機能性のリストを抽出するための別の代替の実装形態は、イメージオブジェクトファイルのチャンクに対して完全性チェックを実施するものでよい。オブジェクトイメージ中の開始アドレスおよび終了アドレスで指定されたあるイメージブロックが、完全性チェックを通らない場合、失敗したセグメントに対応するソフトウェア機能の名称が抽出される。実装された機能に基づいて、失敗したH(e)NB機能性のリストを導出することができる。この導出は、ソフトウェア機能が、一

50

定の H (e) N B 機能性を実装するモジュールに属するので、行うことができる。例えば、UNIX (登録商標) 環境では、「nm」が、オブジェクトファイルにある機能の名称を抽出するための機能性を提供する。この情報は、オブジェクトの記号テーブルから抽出される。

【0044】

妥当性確認方法のためのソフトウェアおよび TRV のダウンロードおよびプロビジョニングについて本明細書に記載する。使われ得る 3 つのプロトコルは、TR069 ベースのアーキテクチャ、OMA (オープンモバイルアライアンス) DM (デバイス管理) ベースのアーキテクチャおよび TCG (trusted Computing Group) IWG (インフラストラクチャワークグループ) ベースのアーキテクチャである。さらに、

10

【0045】

図 3 の TR069 ベースのアーキテクチャは、CPE (顧客構内設備) と自動構成サーバ (ACS) との間の通信を意図した CPE WAN (ワイドエリアネットワーク) 管理プロトコルを記述する。CPE は、H (e) N B にマップし、ACS は、H (e) MS / 修復サーバ / OAM (運用、管理および保守) にマップする。CPE WAN 管理プロトコルは、CPE ソフトウェア / ファームウェアイメージファイルのダウンロードを管理するためのツールを提供し得る。このプロトコルは、バージョン識別、ファイルダウンロード開始 (ACS 開始ダウンロードおよびオプションの CPE 開始ダウンロード)、並びに

20

【0046】

CPE WAN 管理プロトコルは、CPE が実施するべき明示的インストール命令に従って、個々のファイルまたはファイルのパッケージをダウンロードするのにオプションで使われ得る、デジタル署名済みファイル形式も定義し得る。この署名済みパッケージ形式により、ダウンロードされたファイルおよび関連付けられたインストール命令の完全性が確実にされ、ACS オペレータ以外の当事者でよいファイルソースの認証を許可する。ダウンロードされたファイルの完全性検査は、ダウンロードされたファイルに含まれる、個々のモジュールから計算される完全性ダイジェスト (例えば、ハッシュ) と、それに対応する RIM 値との比較に基づき得る。

30

【0047】

CPE WAN 管理プロトコルは、デバイス完全性検査に必要とされる TRV を H (e) N B にダウンロードするのに有用であり得る。このような内容は、ネットワークオペレータの署名鍵でデジタル署名され得る。署名されたパケットを受信すると、H (e) N B は次いで、署名を復号し、受信された TRV の真正性および完全性を検証することができる。コンポーネントが、幾つかのモジュールの順序付き連結として組み立てられるケースでは、TRV は、モジュールに対応する RIM の順序付き連結として組み立てることができる。

【0048】

TRV は、デジタル署名される前に、機密性のために暗号化してもよい。TRV は、デジタル署名された同じパケットの中で、TRV がそれに対して作成されるソフトウェアモジュールバイナリイメージの全体または (最初もしくは最後の) 部分に付加することができる。

40

【0049】

H (e) N B デバイスを取り扱う追加プロシージャについて本明細書に記載する。こうした追加要件およびプロシージャでは、以下の説明において H (e) N B - H (e) MS インタフェースとして識別されるインタフェースを使うことができる。H (e) N B の妥当性確認は、追加プロトコルコンポーネント要件を必要とし得る。H (e) N B - H (e) MS は、SSL / TLS (セキュアソケットレイヤ / 輸送レイヤセキュリティ) をサポートし、H (e) N B と H (e) MS との間の証明書ベースの認証を用いるべ

50

きである。この証明書は、S e G Wへの認証に使われる、同じ証明書でよい。H (e) N B - H (e) M S インタフェース用に T R 0 6 9 ベースのアーキテクチャが使われる場合、C P E 認証のための基本またはダイジェスト認証は、証明書ベースの認証をサポートするように適合される必要があり得る。

【0050】

T R 0 6 9 アーキテクチャに基づく H (e) M S 発見に必要とされ得るプロシージャまたは構造について本明細書に記載する。H (e) N B は、M a n a g e m e n t S e r v e r . U R L パラメータ中のデフォルトの H (e) M S U R L (ユニフォームリソースロケータ)で構成されるべきである。この初期構成は、H (e) N B を分散させている間にオペレータによって、または製造元によって行うことができる。H (e) N B は、認可された管理者によって、L A N (ローカルエリアネットワーク)側 M a n a g e m e n t S e r v e r . U R L 構成をサポートすることができる。H (e) M S U R L は、H T T P S (ハイパーテキスト転送プロトコルセキュア) U R L でよい。ホスティング側 D H C P (動的ホスト構成プロトコル) ベースの H (e) M S U R L アップデートプロシージャは、サポートされなくてよい。値がローカルにアップデートされた場合、H (e) N B は、新規 H (e) M S に接触して、構成ファイルをブートストラップし、密接性(affinity)を確立することができる。U R L は、名称または I P (インターネットプロトコル) アドレスである場合、D N S (ドメインネームシステム) 解決を求め得る。名前の D N S 解決は、複数の I P アドレスを戻す場合があり、そのケースでは、複数の I P を戻してはならないことが確実になるか、または複数の I P が戻された場合は、H (e) N B がランダムに 1 つを選び出すかのどちらかである。

【0051】

T R 0 6 9 アーキテクチャに基づく S e G W 発見について本明細書に記載する。H (e) S U R L と同様、S e G W U R L を、パラメータ (S e c u r e G a t e w a y . U R L) として追加することができる。この U R L は、H (e) N B の場所に基づいて、オペレータによって構成され得る。D H C P によるこのパラメータのアップデートは、サポートすることができない。認可された管理者によるローカルアップデートは実施することができる。

【0052】

A u V および S A V の目的で、T R 0 6 9 、O M A D M、または T C G I W G などのデバイス管理プロトコルを適応させるための追加機構について本明細書にこれ以降で記載する。

【0053】

妥当性確認方法のためにソフトウェアおよび T R V をダウンロードしプロビジョニングする、O M A D M ベースのアーキテクチャについて本明細書に記載する。O M A D M は、O M A D M 作業グループおよび D S (データ同期) 作業グループによって共同で指定されるデバイス管理プロトコルである。O M D D M は、電話、P D A、および他の同様のデバイスなど、小型のフットプリントモバイル機器用に開発されたが、機器と D M サーバとの間のブロードバンドワイヤライン接続性はサポートせず、短距離ワイヤード接続性 (例えば、U S B (ユニバーサルシリアルバス) や R S 2 3 2 C) またはワイヤレス接続性 (G S M (登録商標) (移動体通信用グローバルシステム)、C D M A (符号分割多重アクセス)、W L A N (ワイヤレスローカルエリアネットワーク)、および他のワイヤレス通信システム) のみをサポートし、H (e) N B 用のデバイスプロビジョニングおよび管理プロトコルとして有用であり得る。このことは、コアネットワークに対しては W T R U (ワイヤレス送受信ユニット) としてそれ自体を提示し、共通シリアルゲートウェイ (C S G) およびそれに接続する非 C S G W T R U に対しては基地局としてそれ自体を提示し得る H (e) N B に対して当てはまり得る。

【0054】

O M A D M は、プロビジョニング (初回デバイス構成を含み、特徴を可能/不能にする)、デバイス構成アップデート、ソフトウェアアップグレード、並びに診断報告および

照会などの使用ケースをサポートし得る。OMA DMサーバ側は、こうした機能すべてをサポートすることができるが、デバイスは、オプションで、こうした特徴の全部またはサブセットを実装してもよい。

【0055】

OMA仕様は、小型フットプリントデバイス向けの、上に列挙した特徴を、接続性を制約してサポートするように最適化され得る。この仕様は、それらの仕様の一部として行われる認証プロトコルを用いて（EAP-AKA（`extensible authentication protocol-authentication and key agreement`）などのプロトコルを使用することによって）、統合型セキュリティもサポートし得る。

10

【0056】

OMA DMは、XML（または、より正確には、SyncMLのサブセット）を、データ交換に使うことができる。これは、妥当性確認目的のために、ソフトウェアモジュール用の属性またはH(e)NB用の機能性を定義し伝えるための、標準化可能でありながら柔軟なやり方を提供するのにも有用であり得る。

【0057】

デバイス管理は、DMサーバ（デバイス用の管理エンティティ）とクライアント（管理されるデバイス）との間で起こる。OMA DMは、WAP（ワイヤレスアプリケーションプロトコル）、HTTP、またはOBEX（オブジェクト交換）もしくは同様のトランスポートなどのトランスポートレイヤをサポートする。

20

【0058】

DM通信は、通知または警告メッセージどちらかを用いる、WAP、プッシュまたはSMS（ショートメッセージサービス）など、任意の利用可能方法を用いて、DMサーバによって非同期に開始される。サーバとクライアントとの間で通信をセットアップすることができると、メッセージのシーケンスを交換して、所与のDMタスクを完了することができる。

【0059】

OMA DM通信は、要求応答プロトコルに基づいてよく、このプロトコルでは、要求はDMサーバによってのみ行うことができ、クライアントは、返信メッセージで応答するだけでよい。サーバおよびクライアントは両方とも状態をもち、このことは、特有のシーケンスが原因で交換されるどのデータも、内蔵型認証プロシージャの後でのみ起こり得ることを意味する。

30

【0060】

DM通信は、DMサーバによってのみ開始することができるので、DMを介したSAVの実装には、妥当性確認のためのサーバ照会ベースの手法が求められる場合があり、可能性としては（即座に）、IKE（インターネット鍵交換）v2（デバイスによって開始される）を用いるデバイス妥当性確認プロシージャに続く。異なる幾つかのメッセージタイプは、妥当性確認データ（例えば、失敗したソフトウェアモジュールやデバイス機能性のリスト）のコンペアと見なすことができる。例えば、管理警告メッセージは、デバイスからサーバに送られ得る。或いは、少なくとも1つの管理警告メッセージがデバイスまたはサーバどちらかから伝送された後でデバイスからDMサーバに送られ得る汎用警告メッセージのユーザも、検討され得る。こうした警告メッセージを含む全メッセージは、内容および内容に関するメタデータを指定する際の柔軟性を与えるSyncML（同期マークアップ言語）形式を使うので、妥当性確認情報転送に有用であり得る。DMは、セグメント化データ転送をサポートすることができ、この転送は、アップデートのサイズが大きい場合があるソフトウェアアップデートに有用であり得る。セグメント化データ転送は、このような情報のサイズにより、複数のメッセージへの区分が求められる程十分に大きいケースにおいて、H(e)NBからPVEへの、H(e)NBの、失敗した機能性のリストの転送にも用いることができる。

40

【0061】

50

妥当性確認方法のためのソフトウェアおよびTRVをダウンロードしプロビジョニングする、TCG IWGベースのアーキテクチャについて本明細書に記載する。TCG (trusted Computing Group)、IWG (インフラストラクチャ作業グループ)は、プラットフォーム完全性管理のための詳細な形式およびプロトコルを指定している。完全性測定および報告のための基本的なモデルでは、ネットワークおよびサービスアクセスは、プラットフォームの検証済み状態が条件とされ得る。

【0062】

TCG IWG標準は、H(e)NB SAVまたはAuV用に求められる構造のスーパーセットを提供する。IWG仕様はどれも、そのまま用いることはできない。さらに、IWG仕様を、デバイス妥当性確認の特有の使用ケースにプロファイリングするには、XMLスキーマの修正 (例えば、求められる要素の省略) が求められ、これは、IWG標準からの逸脱を意味する。

【0063】

要求側プラットフォームとネットワーク側検証元との間の基本的な対話を、図4に示す。検証元は、要求側のプラットフォームのコンポーネントそれぞれに関する権威ある情報を探す必要がある (第5のステップで)。つまり、検証元は、メトリックプロバイダによって利用可能にされるプラットフォーム妥当性確認のために、参照測定値を求める。メトリックプロバイダの例は、ハードウェア製造元、ソフトウェアベンダまたは製造元およびベンダの代理の信頼できるプロバイダである。検証元が、要求側のプラットフォームの各コンポーネントを識別し、報告された測定値を、期待される (ベースライン) 参照測定値 (そのコンポーネントに関する) と突き合わせて比較することができると、検証元は、要求側のプラットフォームの信頼レベルを測ることができる。この段階で、検証元は、依頼当事者 (relying party) の所で資源/サービスにアクセスするための、要求側の要望に関して決定を行うことができる。これを、第6のステップに示す。

【0064】

IWG完全性検証アーキテクチャは、検証されたプラットフォーム上でのハードウェアTPM (信頼プラットフォームモジュール) の存在にほとんど依存しないことに留意されたい。特に、標準において指定されるデータ形式は、汎用コンポーネントおよびプラットフォームセキュリティ関連属性を表すことが可能である。

【0065】

所与のコンポーネントにおける技術的信頼をサポートするために、コンポーネント製造元は、コンポーネントの出所に関する情報をもつ、製造元の製品をサポートすればよい。つまり、製造元または信頼できるサードパーティは、そのコンポーネントに関する幾つかの静的参照値を提供しなければならない。コンポーネントに関するこうした静的参照/メトリック値は、参照測定値と呼ばれ、TCG参照マニフェスト (RM) 構造の形で表される。コンポーネント用のマニフェストは、その識別、製造元、モデル番号、バージョン番号、およびそれ以外などの情報を含む。このアプリケーションの目的のために、H(e)NBのコンポーネントの信頼できる参照値 (TRV) は、TCG IWG参照マニフェスト (RM) 構造によって指定され得る。

【0066】

プラットフォームは、妥当性確認される必要があるとき、妥当性確認元 (プラットフォーム検証エンティティ、すなわちPVEなど) に、図5に示すような、プラットフォームのコンポーネントをカバーする1組のスナップショットからコンパイルされた完全性レポートを提供しなければならない。スナップショットは、プラットフォームのすべての関連コンポーネント (および可能性としてはこうしたコンポーネントの下位コンポーネント) についての測定値およびアサーション両方を表す。参照 (ID Ref) は、図6に示すように、完全性レポート中で報告されるコンポーネントに関する情報をポイントするのに使われる。

【0067】

RMに基づく妥当性確認のためのコア要素は、TCG標準に記載されている。柔軟性の

10

20

30

40

50

ために、XML 名前空間が、IWG 形式、例えば、モバイル、または PC クライアントのプラットフォーム固有プロファイル用に使われ得る。

【0068】

相互運用可能な完全性ログ構造は、プラットフォーム特有の符号化を指示するための「ハードウェアアーキテクチャ」タイプ値を定義することによって、幾つかのプラットフォーム特有の制約に対処することができる。タイプ値は、XML 名前空間および XRI など、相互運用可能な名前空間機構を用いる TCG 名前空間によって定義され得る。

【0069】

コアスキーマから拡張によって継承する RM スキーマは、参照を保持するための構造を定義する。RM スキーマは、図 7 に示すように、2 つの情報セットからなるものとして、大まかに理解すればよい。第 1 のものは、個々のコンポーネントについての情報に関し、例えばコンポーネントモデル、名称、バージョン、シリアルナンバーなどの属性をカバーする。この情報は、ComponentIDType 構造に取り込まれる。このコンポーネント特有の周辺情報は、コンポーネント情報の取込み（獲得）に関するメタデータである。このデータは、スキーマにおける IntegrityManifestType 構造で表される。取り込まれるメタデータは、使われる収集（獲得）方法、RM 署名（および関連付けられた署名者／発行元情報）、コンポーネント（ソフトウェア用）に関するダイジェスト値（複数可）、信頼性レベル（confidence level）、行われるアサーション並びにそれ以外を含む。

【0070】

AuV 特有の項目について本明細書に記載する。AuV では、完全性チェックはローカルに実施することができる。したがって、本明細書に記載するデジタル署名またはメッセージ認証コードのどれを使ってもよい。これらは、製造元の私有鍵／共有の秘密を使って、製造元によって署名し、その真正性を、製造元共有の秘密または公開鍵を使ってローカルに検証することができ、コードの完全性をローカルに検証するのに使うことができる。

【0071】

ただし、AuV では、デバイス妥当性確認は、デバイス内部でローカルに実施することができ、情報は、どのネットワークエンティティにも送られない。したがって、妥当性確認に使用するための正確な方法の決定は、製造元に一任され得る。ただし、「完全性アルゴリズムは、SHA-1 と等価またはより優れたセキュリティを与えなければならない」など、最低限のセキュリティ要件を標準化することができる。

【0072】

どのようにして AuV が TRV 証明書管理を実装するかについて本明細書に記載する。システムのコンポーネントは、実際の実装形態に依存するので、デバイス完全性に用いられる複数の機構を調和させる必要がある。これは、TRV として知られる信頼できる参照完全性メトリックを生成するのに用いられる方法に対する最低要件を標準化することによって達成され得る。こうした TRV は、製造元によっても、値にデジタル署名する TTP によっても生成することができる。したがって、情報を編成し、TRV を生成し、分配し、使うための機構が見直される。

【0073】

初回 TRV 証明書初期化について本明細書に記載する。H(e)NB を完全に開発した後、製造元は、ローカル完全性データ初期化を実施する。このプロセスでは、ソフトウェアモジュール名がすべて、デバイス構成データシート中に収集される。構成ファイルに関連したいずれかの工場設定が存在する場合、こうした設定は、デバイス構成データシートにも含まれる。モジュールは、実行可能ファイルであってソースコードではない。構成データの初期プロビジョニングも実施される。デバイス構成データシートスキーマは、標準スキーマに従う。本明細書において提示する XML または ASN.1 スキーマは、ベースラインとして使われ得る。重大度、互換性、段階およびそれ以外についての属性はすべて、デバイスのアーキテクチャに基づいて投入される。

【0074】

図8は、証明書管理アーキテクチャ800を示す。製造元の証明書サーバ805の所で、モジュールエントリ810はすべて、参照完全性メトリックを投入される。完全性方法属性およびTRV属性が投入される。デバイス構成データシートは次いで、私有鍵820を使って製造元によって署名される。データシートは、TTPによって製造元に対して発行されるルート証明書を参照して証明することもできる。このように、参照完全性メトリック(RIM)はTRV830になる。

【0075】

代替アーキテクチャでは、TRVは、TTPによって生成することができる。製造元は、実行可能ファイルと、モジュールすべておよび製造元のサイトで満たすことができる幾つかの投入済み属性を列挙する、部分的に完了されたデバイス構成シートとを提供する。ダイジェストメトリックであるTRVは、TTPによって投入される。TTPは次いで、デバイス構成証明書にデジタル署名する。

10

【0076】

AuVはデバイス内部でローカルに実施されるので、デバイス構成データシートは、デバイス内部で維持することができる。デバイス構成データシートは、認可された当事者によってのみアクセスされ得る安全なメモリ内に保たなければならない。或いは、デバイス構成データシートは、暗号化されなければならない、読み出され、使われるときにH(e)NB内で復号され得る。いずれのケースでも、H(e)NBの信頼できる環境(TrE)のみが、アプリケーションによる読出しアクセスのためにデバイス構成データシートを解放し、またはそれを修正する権限をもつべきである。

20

【0077】

安全なスタートアッププロセスの間、デバイスがコンポーネントのローカル測定を実施すると、生成されたダイジェストは、デバイス構成データシート中で指定された値と比較される。不一致が起きた場合、デバイス完全性の妥当性確認の失敗と解釈される。デバイス構成データシートの完全性は、アクセスされる前に検証されなければならない。デバイス構成データシートの完全性は、データシート中で指定されるいずれか1つまたは複数のコンポーネントの1つまたは複数の完全性チェック失敗の後で検証してもよいであろう。

【0078】

後続TRV証明書アップデートプロシージャについて本明細書に記載する。展開されたH(e)NBシステムにとって、製造元によって新規ソフトウェアバージョンが発行される場合、製造元は、H(e)MS/OAMサーバ/修復サーバに、ソフトウェアモジュールとともにデバイス構成データシートを提供することができる。これは、製造元による「PUSH」動作を実施することによって非同期に行われ得る。このようなPUSHは、オペレータと製造元との間で署名されたサービス合意に基づいてオペレータと製造元との間で合意される、スケジュールされたアップデート/アップグレードに基づいてスケジュールされ得る。

30

【0079】

このようなPUSHに続いて、スケジュールされたときにリポートして、H(e)MS/OAM/修復サーバからソフトウェア/ファームウェア向けの「PULL」動作を実施するようデバイスに命令する、ファームウェアまたはソフトウェアモジュールをアップデートするためのOAMプロシージャまたはTRO69プロシージャが呼び出され得る。暗号化、署名およびノンスは、それぞれ、機密性、完全性、および反射攻撃に対する保護などのセキュリティ側面を提供し得る。

40

【0080】

或いは、ソフトウェアリリーススケジュールに基づくスケジュールされた満了によりデバイス構成データシートが失効すると、H(e)NBは、ファームウェア/ソフトウェアアップデートプロセスをスタートし、OAM/修復サーバからソフトウェア/ファームウェア向けのPULLを開始することができる。或いは、H(e)MSは、ソフトウェアリリースの既知のスケジュール(例えば、製造元から取得される)に基づいて、ソフトウェアアップデートの、スケジュールされたPUSHを実施することもできよう。

50

【0081】

デバイスへのソフトウェア／ファームウェアダウンロードをサポートするTR069またはOMA DMアーキテクチャに基づくプロシージャについて本明細書に記載する。AuVのケースでは、TR069プロトコルは、顧客構内機器の遠隔管理のサポートを提供し得る。このプロトコルは、デバイスソフトウェア／ファームウェアアップデートのサポートも提供し得る。TR069を使用して、H(e)NBデバイスにファームウェア／ソフトウェアアップデートを提供することができる。

【0082】

図9に示すように、認可された管理者によって、またはURLアップデートプロシージャを使用することによってH(e)NB905の所で実施することができる後続アップデートのための、H(e)NB905とH(e)MS910との間のAuVプロシージャ例について本明細書に記載する。H(e)NB905は最初に、H(e)MS発見に関して前述したように、Management Server. URLパラメータ(0)中のデフォルトのH(e)MS URL(ユニフォームリソースロケータ)で構成される。これは、製造元によってプロビジョニングされ得る。H(e)MS910は、TCP(伝送制御プロトコル)接続をオープンする(1)。H(e)NB905とH(e)MS910との間で、SSL(セキュアソケットレイヤ)接続が確立されて、安全な通信が許可される(2)。H(e)MS910は、RPC(リモートプロシージャコール)メソッドSetParameterValuesを開始し、Management Server. URLをアップデートする(3)。アップデートが成功した後、SetParameterValuesResponseが、成功または失敗を示す状況フィールドとともにH(e)NB905によって送られる(4)。H(e)NB905は、H(e)MS URLをアップデートする(5)。

【0083】

H(e)NB-H(e)MSインタフェース用にTR069を使ってファイル転送をサポートするAuVプロシージャについて本明細書に記載する。TR069は、ユニキャストおよびマルチキャストトランスポートプロトコルによってファイル転送をサポートする。ユニキャストプロトコルは、HTTP/HTTPS、FTP(ファイル転送プロトコル)、SFTP(セキュアファイル転送プロトコル)およびTFTP(トリビアルファイル転送プロトコル)を含む。マルチキャストプロトコルは、FLUTE(一方向トランスポートでのファイル配信)並びにDSM-CC(digital storage media command and control)を含む。HTTP/HTTPSのサポートは必須である。TR069をH(e)NB-H(e)MSインタフェースにおけるファームウェア／ソフトウェアダウンロードに適応させるために、HTTP/HTTPSに加えて、FTPS(FTPセキュア)が使用されてもよく、TR069に追加される必要がある。FTPS(FTPセキュアおよびFTP-SSLとしても知られる)は、TLS(トランスポートレイヤセキュリティ)およびSSL暗号プロトコルのサポートを追加する、FTPへの拡張である。H(e)NB-H(e)MSインタフェースはTLS-SSLインタフェースを使用するので、FTPSを、ファイルの転送用に実装することができる。

【0084】

TR069は、ファイルをダウンロードする同じTLS接続を再利用し、並列して存在し得るファイルをダウンロードし、または第1のセッションを解放するための新規接続をスポンするのためのサポートも提供する。ダウンロードが完了した後、シグナリング用のTLS接続が確立される。ファイルをダウンロードするのにHTTP/HTTPSが使われる場合、標準TR069プロシージャを使用することができる。

【0085】

修復サポートのためのAuVプロシージャ例について本明細書に記載する。デバイス完全性チェックがAuVにおいて失敗した場合、ローカル非常フラグを設定することができ、システムは、フォールバックコード(FBC)でリブートする。FBCは、デバイス内

10

20

30

40

50

に安全に格納することができ、安全なスタートアッププロシージャ（またはデバイスの基本的な完全性を保証するのに「本質的」と思われる他の任意のデバイスプロセス）が失敗した場合はロードし実行することができる。FBCは、コアネットワークとの基本的な通信能力を有し、予め指定されたH(e)MSに非常信号を送る能力を有する。H(e)MSは、H(e)MS発見プロシージャによってアップデート済みである場合がある。非常信号の内容は、デバイス上のFBC中に安全に格納することもでき、MNOによってプロビジョニングし、デバイス構成データシートの一部として安全に格納することもできる。非常信号は、デバイス完全性チェック失敗の詳細を示すエラーコード情報要素を含み得る。非常信号を受信すると、ネットワークは、信頼できる参照値を含む完全イメージおよびデバイス構成ファイルをアップデートすることを決定することができる。FTPサーバは、完全イメージ、デバイス構成ファイルおよびインストール命令を含むパッケージファイルを格納する。FTPサーバは、H(e)MSとマージされ得る。

【0086】

このプロシージャは、TRO69プロトコルをサポートするFBCによって遂行することができ、H(e)NB1005、H(e)MS1010およびFTPサーバ1015の間のフローチャート例1000を図10に示す。デバイス完全性チェックが失敗し、信頼のルート(RoT)がH(e)NB1005の所でFBCを起動済みである(0)場合、H(e)NB1005は、予め指定されたH(e)MSサーバ1010へのTCP接続をセットアップする(1)。SSL開始が実施され、および／またはTLS(トランスポートレイヤセキュリティ)がセットアップされる(2)。H(e)NB1005は次いで、H(e)MS1010へのRPCメソッドINFORM、例えば、非常信号を呼び出す。非常信号は、Device ID、Event、MaxEnvelopesおよびCurrentTimeなど、情報要素のどの組合せも含み得る。

【0087】

Device IDは、製造元名と、デバイス製造元のOUI(組織的に一意の識別子)と、シリアルナンバーが該当する製品のクラスを示し、またはTrE IDもしくはH(e)NB IDを示すのにSerialNumber属性を使用させるためにデバイスのシリアルナンバーを示すのに使用することができるProductClassと、特定のデバイスのシリアルナンバーを送り、またはTrE IDもしくはH(e)NB IDを送るのに使われ得るSerial Numberとを含み得る構造である。

【0088】

Eventフィールドは、RPCメソッドInformを実行させたイベントコードを含み得る。新規イベントコード(X_HeNB_FBC_Invoked)は、デバイス完全性チェックが失敗したこと、およびこの非常信号を送るためにFBCが呼び出されていることを示すように定義される必要があり得る。単一のHTTP応答に含まれ得る「SOAPエンベロープ」と呼ばれるパラメータの最大出現回数をACS(例えば、H(e)MS)に対して示すMaxEnvelopes値は、1に設定すればよい。MaxEnvelopeパラメータの値は、1以上になり得る。非常指示は、一度だけ送られることを意図しているので、この値を1に設定することが適切である。CurrentTimeフィールドは、H(e)NB1005に知られている現在日時の値である。したがって、Inform RPCメソッドは、デバイスが完全性チェックに失敗し、ファームウェア／ソフトウェアアップデートを開始するために接続中であることをH(e)MS1010に対して示す。

【0089】

プロシージャ1000の残りはオプションである。H(e)MS1010は、RPCメソッドのダウンロードを呼び出すことができ、ファームウェアまたはソフトウェアおよびデバイス構成データシートの場所のURLを与える(4)。以下のパラメータ値が設定され得る。CommandKeyパラメータは、ある特定のダウンロードを指すのにH(e)NB1005によって使われ得る文字列である。これは、ダウンロードと応答を相関させるのに使われる任意の文字列でよい。FileTypeパラメータは、ファームウェア

／ソフトウェアイメージに対しては「1、ファームウェアアップグレードイメージ」に、デバイス構成データシートに対しては「X__<OUI>__data__sheet」に設定することができる。URLパラメータは、ダウンロードファイルのURLである。HTTPおよびHTTPSがサポートされなければならない。FTPSのサポートも、ダウンロード用に推奨される。Usernameパラメータは、ファイルサーバに対して認証を行うのに、H(e)NB1005によって使われ得る。Passwordパラメータは、H(e)NB1005によって、ファイルサーバに対して認証を行うのに使われ得る。FileSizeパラメータは、ダウンロードされるべきファイルのサイズである。他のパラメータも設定することができる。

【0090】

H(e)NB1005は、FTPサーバ1015に接続し、ファームウェアイメージ（またはソフトウェアイメージ）およびデバイス構成データシートをダウンロードする（5）。FTPサーバ1015の所の情報は、修復情報として示され得る。ダウンロードの完了が成功すると、ゼロ（成功を示す）の値をもつStatus引数を有するDownloadResponse、またはダウンロード要求への失敗応答（失敗を示す）が送られる（6）。成功または失敗したダウンロードを示すための代替的プロシージャがとられてもよい。成功したDownloadResponseの後、H(e)MS1010は次いで、H(e)NB1005内でリブートプロシージャを呼び出すことができる（7）。H(e)NB1005内のRPCハンドラは、ローカル非常フラグをリセットし、正常にブートして、ローカル完全性チェックプロシージャを実施する（8）。署名されたパッケージ形式は、リブートコマンドを含んでよく、このコマンドは、ファームウェアまたはソフトウェアがアップデートされた後でリブートするようH(e)NB1005に命令するのに使われ得る。ファームウェア／ソフトウェアアップデートのプロシージャが首尾よく完了されたことをH(e)MS1010に示すためにTransferComplete RPCメソッドが、H(e)NB1005から呼び出され得る（9）。或いは、SeGWが、成功したファームウェア／ソフトウェアアップデート完了メッセージとしてH(e)MS1010内で翻訳され得る、デバイスが首尾よくブートしたことを示すためのメッセージをH(e)MS1010に送ってもよい。

【0091】

H(e)NBファームウェア／ソフトウェアアップデートに使うことができ、図11に示すファイル形式例1100について本明細書に記載する。ヘッダー1105は、プリアンブル、形式バージョン、並びにコマンドリストおよびペイロードコンポーネントの長さを含む固定長の構造でよい。コマンドリスト1110は、パッケージに含まれるファイルを抽出しインストールするように実行することができる一連の命令を含む。各コマンドは、TLV（タイプ、長さ、値）の形でよい。署名フィールド1115は、ゼロ以上のデジタル署名のセットを含み得るPKCS（公開鍵暗号技術標準）#7デジタル署名ブロックを含み得る。ペイロードファイル1120は、コマンドリスト1110中の命令に従ってインストールされるべき1つまたは複数のファイルを含み得る。ファームウェア／ソフトウェアアップデートファイルに加えて、デバイス構成データシートも、署名されたパッケージ形式でパッケージ化される。

【0092】

ストレージ分類器の要件をサポートするために、以下の新規H(e)NB特有のコマンドを追加することができる。すなわち、1）安全な不揮発性メモリに格納する（TRVや構成データシートなどのデータの場合）、2）不揮発性ストレージに格納する、または3）揮発性ストレージに格納することができる。

【0093】

図12は、SAV用のネットワークアーキテクチャ例1200を示す。H(e)NB1205が、ユーザ機器1210用のゲートウェイとして作用して、コアネットワーク1220への通信リンク1215を介して通信する。H(e)NB1205は、安全でない通信リンク1215を介してSeGW1225と対話する。SeGW1225は、認証され

10

20

30

40

50

たH (e) NBが、コアネットワーク1220にアクセスすることを許可することができる。H (e) MS1230が、H (e) NB管理サーバとして作用し、修復のサポートを提供する。H (e) MS1230は、H (e) NB1205を管理するための標準プロトコルをサポートし得る。プラットフォーム妥当性確認エンティティ (PVE) 1235が、H (e) NB1205内の、ある機能性セットが失敗したときにとられるべきアクションを定義するポリシーを格納する。こうした失敗した機能性は、SAVプロセス中にH (e) NB1205によって報告される。OAM1240は、運用、管理および保守サーバである。H (e) MS1230およびPVE1235は、別個のエンティティとして示してあるが、単一のネットワークエンティティとして、互いとマージしてもよい。このようなマージされたエンティティは、ネットワークオペレータごとに単一のノードでもよく、オペレータごとに複数のノードでもよい。

10

【0094】

SAVに関するプロシージャについて本明細書に記載する。要約すると、デバイス妥当性確認プロシージャを実施し始める前に、H (e) NBのTrEは最初に、ブートコード、フォールバックコード (FBC)、SeGW用の基本的な通信コード、およびH (e) NBがH (e) MSにアクセスすることを可能にするプロシージャを実施するコードなどだが、それに限定されない、予め指定された特定のコンポーネントの完全性のチェックを実施する。このステップでは、コンポーネントの完全性の検証は、完全性測定から得たダイジェスト出力を、デバイス構成データシート中の指定された値と比較することによって、ローカルに実施することができる。コンポーネントは、完全性検証を通った場合、ロードされ実行される。

20

【0095】

それ以上のチェックは、TrE自体またはTrEの外部だがTrEによって完全性が保護される、H (e) NB内の測定側コンポーネントのどちらかによって起こり得る。このような後期段階チェックでは、他のコンポーネント、構成、またはH (e) NBの残りのパラメータの完全性が、それらがロードされ、もしくはスタートされるとき、または、それらが測定側コンポーネントにとって使用可能な場合は常に、他の、予め定義されたランタイムのイベント時にチェックされ得る。このステップで、完全性チェックの検証はローカルに実施することができる。

【0096】

H (e) NBは次いで、SeGWとのIKEv2 (インターネット鍵交換) セキュリティアソシエーションの確立を試みることができる。このプロセスで、H (e) NBは、SeGWに対してそれ自体を認証し、SeGWの真正性を検証する。これは、証明書交換および証明書認証によって実施することができる。認証が成功した場合、TrEは、コンポーネントの失敗によって影響を受ける、失敗した機能性のリストをコンパイルすることによって、ローカル完全性検証の結果をPVEに伝える。TrEは次いで、メッセージに署名する (TrEによって保護された署名鍵を使って、したがってメッセージの完全性を保護する) ことができ、こうすることにより、完全性測定および検証、並びに失敗した機能性のリストの (PVEへの) 報告を実施したH (e) NBのコア部が、それに対して実施された完全性チェックを通り (例えば、信頼のルート (RoT) によって)、したがって署名鍵を使い、署名操作を実施することができ、或いは秘密署名鍵の使用により本質的に信頼されることをアサートする。

30

40

【0097】

図13A、13Bは、H (e) NB1305、SeGW1310およびPVE1315によって実施されるSAVプロシージャ例1300を示す。コンポーネント1およびコンポーネント2モジュールのローカル完全性の妥当性確認の後、モジュールがロードされ実行される。コンポーネント3モジュールのデバイス完全性チェックの結果および検証結果が、H (e) NB1305によってSeGW1310に送られて、PVE1315にフォワードされる (0)。

【0098】

50

H (e) N B 1 3 0 5 は、 I K E _ I N I T メッセージを送って、暗号アルゴリズム用のセキュリティパラメータ索引、バージョン番号、 I K E v 2 フラグ、ディフィーヘルマン値およびイニシエータノンスを含む I K E v 2 セキュリティアソシエーションの確立を開始することができる (1) 。 S e G W 1 3 1 0 は、 I K E _ I N I T 要求メッセージに対する I K E _ I N I T 応答を送ることができる (2) 。 S e G W 1 3 1 0 は、 H (e) N B 1 3 0 5 から暗号スイートを選ぶことができ、ディフィーヘルマン交換を完了する。 H (e) N B 1 3 0 5 は、その証明書を、 I K E _ A U T H _ R E Q に入れて相互認証のために送ることができる (3) 。これは、失敗した機能性のリストの形の完全性検証の結果も含み得る。ローカル完全性検証が成功した場合は、このような失敗した機能性のリストは含まれない。この場合は、空リストが送られる。コンポーネント、モジュールおよび機能性の間の関係については、本明細書に記載した。

10

【 0 0 9 9 】

S e G W 1 3 1 0 は、 H (e) N B 1 3 0 5 の認証資格を評価することができ、存在する場合は P V E 1 3 1 5 に送られるべき機能性 I D のリストを抽出する (4) 。認証評価が成功した場合、 S e G W 1 3 1 0 は、このことを、 H (e) N B 1 3 0 5 に対して示す (5 s) 。 S e G W 1 3 1 0 は、それ自体の証明書を、応答に入れて H (e) N B に送ることもできる。認証が失敗した場合、このことは、 H (e) N B 1 3 0 5 に伝達される (5 f) 。

【 0 1 0 0 】

認証が成功し、失敗した機能性のリストが I K E _ A U T H メッセージに含まれていた場合、 S e G W 1 3 1 0 は、失敗した機能性のリストを、 H (e) N B I D とともに P V E 1 3 1 5 にフォワードする (6) 。リストがない場合、空リストが P V E 1 3 1 5 に送られる。失敗した機能性のリストに基づいて、 P V E 1 3 1 5 は、デバイスの検疫、完全アクセスの提供、部分アクセスの提供、またはオプションでデバイス修復のための H (e) M S 介入の要求など、とられるべきアクションを決定することができる (7) 。 P V E 1 3 1 5 は、影響を受けたその機能性が決定的ではなく、したがって H (e) N B 1 3 0 5 が機能し得ると判断した場合、この判断を S e G W 1 3 1 0 に対して示して、デバイスがネットワークにアクセスすることを許可する (8 s) 。 S e G W 1 3 1 0 は、 P V E 1 3 1 5 によって実施されたデバイス完全性評価の結果を指示する。失敗したモジュールが決定的でない場合、 P V E 1 3 1 5 は、 H (e) N B 1 3 0 5 にネットワークへの完全

20

30

【 0 1 0 1 】

修復がサポートされる場合、 P V E 1 3 1 5 は、 H (e) M S 1 3 2 0 に指示を送って、メッセージにおいて H (e) N B I D によって識別されたデバイスに対する修復をスタートする (8 f _ 1) 。 P V E 1 3 1 5 は、失敗したモジュールのリストも含み得る。失敗した機能性のリストおよびデバイス特有の構成データシートに基づいて、 H (e) M S 1 3 2 0 は、求められるファームウェアまたはソフトウェアアップデートを決定する。修復がサポートされる場合、 P V E 1 3 1 5 は、 H (e) N B 1 3 0 5 に指示を送って、 H (e) M S 1 3 2 0 が開始した修復を準備することができる (8 f _ 2) 。 P V E 1 3 1 5 からの応答に基づいて、 S e G W 1 3 1 0 は、アクセスを制限し、結果を H (e) N B 1 3 0 5 に知らせることができる (9 f) 。システムは、 F B C モードでリポートして、デバイス開始修復をスタートする (1 0) 。このステップは、リポートは、修復用の T R 0 6 9 プロトコルを使って H (e) M S 1 3 2 0 によって扱われ得るので、オプションでよい。

40

【 0 1 0 2 】

50

S A VのためのH (e) M SおよびP V E発見プロシージャについて本明細書に記載する。H (e) N Bは、P V E、H (e) M SおよびO A MのI Pアドレスを含む、工場出荷時設定で構成され得る。こうした設定は、図9に示したように、T R O 6 9プロトコルにサポートされるR P CメソッドS e t P a r a m e t e rおよびG e t P a r a m e t e rを使って、T R O 6 9プロトコルを使うH (e) M Sによって再構成することもできる。プロシージャは、P V Eのアドレスを変更するのにも用いられ得ることに留意されたい。M a n a g e m e n t S e r v e r . U R Lパラメータ (P l a t f o r m V a l i d a t i o n S e r v e r . U R L) に同様の追加パラメータが、H (e) N Bの所でP V E U R Lを維持するために定義され得る。同様に、P l a t f o r m V a l i d a t i o n S e r v e r . U R Lの工場設定は、製造時に予め構成され、その後でT R O 6 9によってアップデートされ得る。

10

【0103】

S A Vのための完全性方法およびプロシージャについて本明細書に記載する。S A Vにおいて、デバイス完全性チェックはローカルに実施することができる。完全性チェックの結果は、失敗した機能性のリストの形でP V Eに渡すことができる。したがって、本明細書に記載する完全性チェック方法のいずれも、例えば、原文明細書の段落[0038]～[0040]に示したように用いることができる。完全性チェックは、ネットワークエンティティによって実施されるのではない。したがって、妥当性確認に使用するための正確な完全性方法の決定は、製造元に一任され得る。ただし、「完全性方法は、S H A - 1と等価またはより優れたセキュリティを提供しなければならない」など、最低限のセキュリティ要件は標準化することができる。

20

【0104】

S A VにおけるT R V証明書管理に用いられ得る機構について本明細書に記載する。S A Vをサポートするインタフェースおよびメッセージについて、最初に記載する。P V E - S e G Wインタフェースは、二地点間プロトコル (P P P) を使用することができる。P P Pは、認証、暗号化および圧縮のサポートを提供し得る。或いは、T L S / S S L (トランスポートレイヤセキュリティ / セキュアソケットレイヤ) を使用してもよい。

【0105】

P V E - S e G Wインタフェースを介して送ることができる複数のメッセージがある。例えば、H (e) N B _ I n t e g r i t y _ I n f o r m a t i o nメッセージは、I K E v 2 N O T I F Yメッセージに入れて、H (e) N BによってS e G Wに送られるとともにS e G Wによって抽出される、失敗した機能性のリストを含み得る。このメッセージの内容の例を、テーブル7に示す。

30

【0106】

【表 7】

情報要素	説明
H(e)NB ID	H(e)NBの一意の識別子またはTrE IDを含む。
(オプション)完全性チェックされた全機能性のリスト	(オプション)このリストは、TLV形式であり、チェックされた機能性すべてのリストを含み、そうすることによって、デバイスに対して実施される完全性検査の限度/範囲を示す。このリストは、完全性検査の限度/範囲が、検証元(例えば、PVE)に前もって知られていない場合にのみ送られる。 (代替)或いは、およびやはリオプションで、完全性がチェックされなかった機能性のリストも、チェックされた機能性のリストの代わりに送ることができる。このような代替的リストは、チェックされていない機能性のリストが、チェックされた機能性のリストより短い場合は、サイズがより小さくてよい。この方法は、チェックされ得る全機能性のリスト全体が、検証元に既に知られている場合に作用するに過ぎない。
失敗した機能性のリスト	このリストは、TLV形式であり、失敗した機能性のリストを含む。このリストは、どの機能性も失敗していないことをH(e)NBが報告した場合は空でよい。報告は、信頼できる完全性検証済みコードで生成され、したがって安全なスタートアッププロセスにより信じられることに留意されたい。
ノンス/メッセージシーケンス番号	ノンスまたはメッセージシーケンス番号は、要求と応答を関連付けるものである。

テーブル7

【0107】

H(e)NB_Integrity_Informationメッセージに対する応答は、テーブル8に示すH(e)NB_Validation_Resultである。

【0108】

10

20

30

【表 8】

情報要素	説明
H(e)NB ID	H(e)NBの一意の識別子またはTrE IDを含む。
ノンス/メッセージシーケンス番号	要求と応答を関連付けるためのH(e)NB_Integrity_Information中で与えられるノンス。
SeGWアクション	SeGWが実施し得るアクションは、以下を含む。 1. 完全アクセスの許可 2. H(e)MSのみへのアクセスの許可 3. 検疫 4. アクセスの却下
H(e)NBアクション	こうしたアクションは、IKEv2 NOTIFYメッセージに入れてH(e)NBにフォワードされる。H(e)NBアクションは、以下であり得る。 1. 完全アクセスの許可(アップデートは必要とされず、エラーは起こらない) 2. 完全アクセスの許可(アップデートがスケジュールされ、重大度4のエラーが起こる) 3. 部分アクセスの許可(アップデートがスケジュールされ、重大度2のエラーが起こる) 4. H(e)MSのみへのアクセス(即座の修復を準備し、重大度3のエラーが起こる) 5. シャットダウン(ローカルエラーコード表示を伴うシャットダウン、管理者はシステムを個人的に解決する、重大度1のエラー)

10

20

テーブル8

【0109】

両方ともネットワークエンティティなので、PVE-H(e)MSインタフェースは、PPPにも基づき得る。或いは、TLS/SSLも使用することができる。一例では、PVEおよびH(e)MSは、1つのエンティティでよい。このインタフェースを介したメッセージ例を、テーブル9に示す。

30

【0110】

【表 9】

情報要素	説明
H(e)NB ID	H(e)NBの一意の識別子またはTrE IDを含む。
(オプション)完全性チェックされた全機能性のリスト	(オプション)このリストは、TLV形式であり、チェックされた機能性すべてのリストを含み、そうすることによって、デバイスに対して実施される完全性検査の限度/範囲を示す。このリストは、完全性検査の限度/範囲が、検証元(例えば、PVE)に前もって知られていない場合にのみ送られる。 (代替)或いは、およびやはりオプションで、完全性がチェックされなかった機能性のリストも、チェックされた機能性のリストの代わりに送ることができる。このような代替的リストは、チェックされていない機能性のリストが、チェックされた機能性のリストより短い場合は、サイズがより小さくてよい。この方法は、チェックされ得る全機能性のリスト全体が、検証元に既に知られている場合に作用するに過ぎない。
失敗した機能性のリスト	このリストは、TLV形式であり、失敗した機能性のリストを含む。機能性IDについて本明細書に記載する。リストがNULLの場合、このことは、H(e)NBが全完全性チェックを通ったことを示し得る。
H(e)MSアクション指示	これは、デバイス完全性の妥当性確認が実施され、その結果H(e)MSが幾つかのアクションを実施し得ることをH(e)MSに対して示す。以下のアクションを実施することができる。 1. 即座の修復 2. 修復のスケジューリング 3. 管理者介入の要請

テーブル9

【0111】

或いは、PVEは、失敗した機能性のリストを（または、オプションで、完全性チェックされた全機能性のリスト、もしくは完全性チェックされなかった全機能性のリストも）単に送るだけでよく、H(e)MSが、アクション自体を決定する。これを、テーブル10に示す。即座の修復、修復のスケジュール、および管理者介入の要請というアクションが、H(e)MSによって実施され得る。

【0112】

10

20

30

40

【表 10】

情報要素	説明
H(e)NB ID	H(e)NBの一意の識別子またはTrE IDを含む
(オプション)完全性チェックされた全機能性のリスト	(オプション)このリストは、TLV形式であり、チェックされた機能性すべてのリストを含み、そうすることによって、デバイスに対して実施される完全性検査の限度/範囲を示す。このリストは、完全性検査の限度/範囲が、検証元(例えば、PVE)に前もって知られていない場合にのみ送られる。(代替)或いは、およびやはりオプションで、完全性がチェックされなかった機能性のリストも、チェックされた機能性のリストの代わりに送ることができる。このような代替的リストは、チェックされていない機能性のリストが、チェックされた機能性のリストより短い場合は、サイズがより小さくてよい。この方法は、チェックされ得る全機能性のリスト全体が、検証元に既に知られている場合に作用するに過ぎない。
失敗した機能性のリスト	このリストは、TLV形式であり、失敗した機能性のリストを含む。機能性IDについては、上のセクションに記載した。リストがNULLの場合、このことは、H(e)NBが全完全性チェックを通ったことを示し得る。

テーブル10

【0113】

S A Vに関するH (e) N Bアーキテクチャおよび機能性について本明細書に記載する。H (e) N Bアーキテクチャは、外部T r E完全性チェックを含み得る。H (e) N BのT r Eは、完全性検証のタスクが、T r Eの責任であった、コンポーネントの完全性検証のタスクを、実装されたハードウェアおよび／またはソフトウェアでよい外部エンティティに委任することができる。このようなケースは、T r Eが十分に速くない場合、またはデバイス完全性チェックを実施するのに十分な資源をもたない場合に用いられ得る。このようなケースでは、T r Eは、デバイス完全性の妥当性確認のタスクを始める予定のハードウェアおよび／またはソフトウェアエンティティの完全性および真正性を検証する。検証が成功した後、T r Eは、外部完全性チェックが、タスクを実施し、結果および測定データをT r Eに報告することを許可する。

【0114】

H (e) N Bエンティティは、様々なイベント、レポートおよびネットワークとの通信にタイムスタンプを与えるためのローカルタイムサーバを有し得る。このようなタイムサーバは、N T P (ネットワークタイムプロトコル) を使って、時間と同期することができる。タイムサーバコードおよびN T Pコードも、T r Eまたは外部T r E完全性チェックによって実行される前に完全性検証され得る。

【0115】

H (e) N Bアーキテクチャは、妥当性確認および認証のバインドも提供し得る。妥当性確認と認証との間のバインドは、A u Vのケースでの妥当性確認および認証のバインドに使われる機構に加えて、I K E v 2セッション、すなわち、完全性チェックを通過したときのみの、敏感鍵および認証機能性のリリースによって提供され得る。S A Vにおける

認証証明書およびローカル妥当性確認の結果は、IKEv2 IKE__AUTH__REQメッセージに入れて送ることができる。SeGWは、失敗したモジュールのリストをフィルタリングして選別し、PVEにフォワードする。このようなリストがメッセージに含まれない場合、SeGWは、この情報をPVEに中継する。PVEは、今後のアクションを決定し、結果をSeGWに対して、一部のケースではH(e)MSに対しても示す。

【0116】

代替的バインド方法では、H(e)NBは、鍵ペアを予め装備し、このペアの私有部は、H(e)NBのTrEの内側に安全に格納され、公開部は、H(e)NBにとって使用可能にされる。H(e)NBの製造元は、この鍵ペアを生成し、したがって私有および公開鍵をプロビジョニングすることができよう。暗号手段によって妥当性確認および認証のバインドを生じるために、H(e)NBは、AAAサーバから受信する（ここで、AAAサーバは、秘密ベースの計算された認証資料を計算し、AAAサーバに返送するよう、H(e)NBに要求する）メッセージ（例えば、IKE__AUTH応答メッセージ）を、証明書から得た公開鍵で暗号化し、暗号化データをTrEにフォワードする。TrEは次いで、データを復号し、AAAに対してH(e)NBの識別の真正性を検証するのに必要とされる秘密ベース認証資料（例えば、対称認証が用いられる場合はEAP-AKA RESパラメータ、または証明書ベースの認証が用いられる場合は私有鍵の使用に基づくAUTHパラメータなど）を計算する。

【0117】

代替的バインド方法では、H(e)NBのIKEv2ベースのデバイス妥当性確認アプリケーションによって使われる、TrEの鍵および他の敏感な計算能力は、成功したローカル完全性チェック結果がH(e)NBのTrEに知られない限り、このようなアプリケーションに対してアクセス可能にされない。

【0118】

H(e)NBおよびPVEに格納されているポリシー仕様について本明細書に記載する。H(e)NBデバイス構成ファイルは、本明細書において詳しく記載した、機能性ID、コンポーネントIDおよびモジュールIDなどの属性を記述する、H(e)NBに格納されているポリシーを記述する。デバイス構成シートは、製造時に初期化される。AuVのためのこの情報の初期化および後続アップデートのプロシージャは、本明細書に記載済みであり、SAVケースに適用可能である。

【0119】

PVEポリシー構成ファイルは、失敗した機能性と、SeGWアクション、H(e)NBアクション、およびH(e)MSアクションとの間のマッピングを含み得る。失敗した機能性のリストに基づいて、PVEは、H(e)NB、SeGWおよびH(e)MSによってとられるべきアクションを決定し得る。テーブル11は、こうしたアクションを定義する。

【0120】

10

20

30

【表 1 1 - 1】

失敗した機能性の説明	H(e)NBアクション	SeGWアクション	H(e)MSアクション
安全なブートローダ	シャットダウン	検疫	管理者介入
TrE	シャットダウン	検疫	管理者介入
完全性の妥当性確認エンジン	シャットダウン	検疫	管理者介入
フォールバックコード	シャットダウン	検疫	管理者介入
オペレーティングシステム	シャットダウン	検疫	管理者介入

【 0 1 2 1】

H(e)MSサブシステム	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
Uuインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
Iuhインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HGmインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HUtインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
S1-MMEインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
S1-Uインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
I2(SIP)インタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
Iu-CSインタフェース	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
Iu-PSインタフェース	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
E, Nc, Nbインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
RUAサービス	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HNBAPサービス	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HNB GW発見	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HNB登録	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
HNB用WTRU登録	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
アクセス制御管理	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復

10

20

30

【 0 1 2 2 】

時間管理	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
CSG管理	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
移動管理	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
NASノード選択機能	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
ページング最適化	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
トランスポートアドレスマッピング	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
請求	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
緊急サービス	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
QoS管理	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
ローカルIPアクセス	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復

10

20

【 0 1 2 3 】

【表 1 1 - 2】

管理されるリモートアクセス	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
旧来のGN用のHNBサポート	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
着信ハンドオーバーサポート	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
ローミング	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
MSC SGSNへのSCCP無接続通信	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
OAMサブシステム	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
表示サブシステム	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
USIMサブシステム	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
HPMサブシステム	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
IMS関係動作	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
IP-PABXインタフェース			
セキュリティ機能	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
RAB管理	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
無線資源管理	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
Iuリンク管理	H(e) MSのみへのアクセス	H(e) MSのみへのアクセス	即座の修復
IuUプレーン(RNL)管理	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
Iu調整機能	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
プロビジョニング機能	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
ハードウェアの異常	シャットダウン	検疫	管理者介入

テーブル11

【0 1 2 4】

S A Vにおける修復をサポートする方法について本明細書に記載する。修復をサポートするために、H (e) N Bは、H (e) M Sと対話する。この接続は、S e G W経由でも、T L S / S S Lを使うインターネットを介して直接でもよい。安全なスタートアッププロセス中に、デバイス完全性チェックが、製造元によって予め指定され、T r E用のコードとともに、認証およびS e G Wとの通信に必要なコードを含む段階 1 または段階 2 コードに関して失敗した場合、F B Cが実行され、修復が試みられる。

【0 1 2 5】

図14は、H(e)NB1405、H(e)MS1410およびFTPサーバ1415が関与するSAV修復のためのフローチャート例1400を示す。デバイス完全性チェックが失敗した場合、また、FBCを使ってRotが起動した(0)後、H(e)NB1405は、予め指定されたH(e)MSサーバ1410への接続を(例えば、TCP接続を使用して)セットアップする(1)。次いで、SSL開始が実施され、および／または次いで、TLSがセットアップされる(2)。H(e)NB1405は次いで、H(e)MS1410とともにRPCメソッドInform(例えば、非常信号)を呼び出す(3)。非常信号は、Device ID、Event、MaxEnvelopesおよびCurrentTimeを含み得る。

【0126】

10

デバイスIDは、製造元名と、デバイス製造元のOUI(組織的に一意の識別子)と、シリアルナンバーが該当する製品のクラスを示すのに使用され、またはTrE IDもしくはH(e)NB IDを示すのにSerialNumber属性を使用させるために、デバイスのシリアルナンバーを示すのに使用することができるProductClassと、特定のデバイスのシリアルナンバーを送るのに使うことができ、またはTrE IDもしくはH(e)NB IDを送るのに使うことができるSerial Numberフィールドとを含み得る構造である。

【0127】

20

Eventフィールドは、RPCメソッドInformを実行させたイベントコードを含み得る。TRO69をSAV修復に適応させるために、デバイス完全性チェックが失敗したこと、およびこの非常信号を送るためにFBCが呼び出されたことを示すための新規イベントコード(X_HeNB_FBC_Invoked)が定義される必要があり得る。MaxEnvelopes値は、1に設定される。この値は、無視してよいが、1に設定される。CurrentTimeフィールドは、H(e)NB1405に知られている現在の日時の値に設定される。

【0128】

30

Inform RPCメソッドは、デバイスが完全性チェックに失敗し、ファームウェアアップデートを開始するために接続中であることを、H(e)MSに対して示す。H(e)MSは次いで、RPCメソッドUploadを呼び出して、失敗した機能性のリストおよびエラーコードの製造元固有リストをアップロードするよう、H(e)NBに指示する(4)。こうしたエラーコードは、完全性チェックに失敗したコンポーネントに対応するソフトウェアモジュールを指すこともでき、またはデバッグ特有のエラーコードを含み得る。ファイルがアップロードされなければならないFTPサーバ1415のURLが与えられる。FTPサーバ1415は、製造元によって維持され得ることに留意されたい。FTPサーバ1415は、製造元によって提供される修復サーバでよい。

【0129】

40

H(e)MS1410は、メッセージPrepare_For_Uploadを送ることによって、失敗した機能性のリストのアップロードを準備するよう、FTPサーバ1415に指示する(5)。H(e)NB1405は次いで、HTTP/HTTPS/FTPSプロシージャを呼び出して、失敗した機能性のリストを含むファイルをアップロードする(6)。ファイル受信の後、FTPサーバ1415またはH(e)MS1410は、H(e)MSがアップロードされたファイルを収集すると、求められるパッチまたはファームウェア/ソフトウェアアップデートを評価して、問題を解決する(6a)。失敗した機能性のリストを含むファイルが、FTPサーバ1415にアップロードされた場合、求められるパッチの評価の後で、FTPサーバ1415は、Download_Package_ReadyメッセージをH(e)MSに送る(7)。H(e)MSが、アップロードされたファイルを収集済みであった場合、このメッセージは求められない。或いは、このメッセージは、H(e)MS1410およびFTPサーバ1415の機能性がマージされる場合は求められなくてもよい。

【0130】

50

或いは、情報は、PVEから直接受信することができ、ステップ1から5は必要とされなくてもよい。

【0131】

H(e)MS1415は次いで、RPCメソッドDownloadを呼び出し、ファームウェアまたはソフトウェアおよびデバイス構成データシートの場合のURLを与える(8)。以下のパラメータ値を設定することができる。CommandKeyパラメータは、H(e)NB1405によって、ある特定のダウンロードを指すのに使われ得る文字列であり、任意の文字列でよい。このパラメータは、ダウンロードと応答を相関させるのに使われる。FileTypeパラメータは、ファームウェアイメージの場合は「1 ファームウェアアップグレードイメージ」に、デバイス構成データシートの場合は「X__<OU I>__data__sheet」に設定され得る。URLパラメータは、ダウンロードファイルのURLである。HTTPおよびHTTPSがサポートされなければならない。FTPのサポートは、ダウンロード用にも推奨され得る。Usernameパラメータは、H(e)NB1405によって、FTPサーバ1415に対して認証を行うのに使われ得る。Passwordパラメータは、H(e)NB1405によって、FTPサーバ1415に対して認証を行うのに使われ得る。FileSizeパラメータは、ダウンロードされるべきファイルのサイズである。他のパラメータも、TR069プロトコル要件に従って設定され得る。

【0132】

H(e)NB1405は、FTPサーバ1415に接続し、ファームウェアまたはソフトウェアイメージおよびデバイス構成データシートをダウンロードする(9)。ダウンロードの完了が成功すると、値がゼロ(成功を示す)のStatus引数をもつDownloadResponse、またはDownload要求に対する障害応答(失敗を示す)が送られ得る(10)。本明細書に記載する代替的プロシージャに従って、成功または失敗したダウンロードを示してもよい。

【0133】

成功したDownloadResponseの後、H(e)MS1415は次いで、H(e)NB1405内でRebootプロシージャを呼び出す(11)。H(e)NB1405内のRPCハンドラは、ローカル非常フラグをリセットし、正常にブートして、上述したようにローカル完全性チェックプロシージャを実施する(11a)。署名されたパッケージ形式は、ファームウェアまたはソフトウェアがアップデートされた後で、リポートするようH(e)NB1405に命令するのに使われるリポートコマンドを含み得る。

【0134】

オプションで、TransferComplete RPCメソッドをH(e)NBから呼び出して、ファームウェア/ソフトウェアアップデートのプロシージャの完了が成功したことをH(e)MSに対して示すことができる(12)。或いは、SeGWは、H(e)MSにメッセージを送って、デバイスがブートに成功したことを示すことができ、このメッセージは、H(e)MSによって、成功したファームウェアまたはソフトウェアアップデート完了メッセージとして翻訳され得ることに留意されたい。

【0135】

図15は、PVEによるSAV修復の実施のためのフローチャート1500を示す。このプロシージャには、H(e)NB1505、SeGW1510、PVE1515、H(e)MS1520およびFTPサーバ1525が関与する。安全なスタートアッププロセス中、段階1コードおよび段階2コードが完全性チェックを通り、ロードされ実行され、認証の実施が成功した場合、H(e)NB1505は、SeGW1510と通信して、ローカル完全性チェックの結果をIKEv2メッセージに入れて送ることができる(1)。H(e)NB1505は、失敗した機能性のリストおよび製造元固有エラーコードのリストを、図16に示すIKEv2 NOTIFYメッセージ1600に入れてSeGW1510に送る。

【0136】

SeGW1510は次いで、ローカル完全性チェックの結果を、失敗した機能性のリストおよび／またはエラーコードの製造元固有リストを含み得るH(e)NB_Integrity_Informationメッセージに入れて送ることができる(2)。受信された情報に基づいて、PVE1515は、SeGWアクションおよびH(e)NBアクションを含み得るH(e)NB_Validation_ResultメッセージでSeGW1510に応答することができる(3)。SeGW1510は、H(e)NBアクションをH(e)NB1505にフォワードしてよい(5)。H(e)NBは、それに従って準備を行い、また、修復の準備をローカルに行ってもよく、何のアクションをとらなくてもよい。

【0137】

受信された情報に基づいて、PVEは、失敗した機能性のリスト、エラーコードの製造元固有リスト、H(e)MSアクション(複数可)およびH(e)NB_IDを含み得るH(e)NB_Validation_ResultメッセージをH(e)MS1520に送ってもよい(4)。PVE1515によってH(e)MS1520に送られたアクションに基づいて、H(e)MS1520は、修復アップデートまたは即座のアップデートをスケジュールすることができる。両方のケースにおいて、H(e)MS1520は、製造元固有修復FTPサーバにリストを送る。

【0138】

H(e)MS1520は、失敗した機能性のリスト、H(e)NB_ID、およびエラーコードの製造元固有リストを含み得るH(e)NB_Validation_ResultメッセージをFTPサーバ1525にフォワードしてよい(4a)。FTPサーバ1525は、ファームウェア／ソフトウェアダウンロードファイルを評価し、ダウンロードパッケージを準備することができる(4b)。FTPサーバ1525は、Download_Package_ReadyメッセージをH(e)MS1520に送る。H(e)MS1520が、アップロードされたファイルを収集した場合、このメッセージは求められなくてよい。或いは、このメッセージは、H(e)MS1520とFTPサーバ1525がマージされている場合は送られなくてもよい。

【0139】

H(e)MS1520は次いで、RPCメソッドDownloadを呼び出し、ファームウェア／ソフトウェアおよびデバイス構成データシートの場合のURLを与える(7)。以下のパラメータ値を設定することができる。CommandKeyパラメータは、H(e)NB1505によって、ある特定のダウンロードを指すのに使われ得る文字列であり、ダウンロードと応答を関連させるのに使われ得る任意の文字列でよい。FileTypeパラメータは、ファームウェア／ソフトウェアイメージの場合は「1 ファームウェアアップグレードイメージ」に、デバイス構成データシートの場合は「X_<OUI>_data_sheet」に設定することができる。URLは、ダウンロードファイルのURLである。HTTPおよびHTTPSがサポートされなければならない。FTPのサポートは、ダウンロード用にも推奨される。Usernameパラメータは、H(e)NB1505によって、ファイルサーバに対して認証を行うのに使われ得る。Passwordパラメータは、H(e)NB1505によって、ファイルサーバに対して認証を行うのに使われ得る。FileSizeパラメータは、ダウンロードされるべきファイルのサイズである。他のパラメータは、TR069プロトコル要件に従って設定することができる。

【0140】

H(e)NB1505は、FTPサーバ1515に接続し、ファームウェア／ソフトウェアイメージおよびデバイス構成データシートをダウンロードする(8)。ダウンロードの完了が成功すると、値がゼロの(成功を示す)Status引数をもつDownloadResponse、またはダウンロード要求に対する障害応答(失敗を示す)がH(e)MS1520に送られる(9)。TR069に記載されている代替的プロシージャに従って、成功または失敗したダウンロードを示すこともできる。

10

20

30

40

50

【0141】

成功したダウンロード応答の後、H(e)MS1515は次いで、H(e)NB1505内でRebootプロシーダを呼び出す(10)。H(e)NB1505内のRPCハンドラは、ローカル非常フラグをリセットし、正常にブートして、上で示したようにローカル完全性チェックプロシーダを実施する(10a)。或いは、署名されたパッケージ形式は、ファームウェア/ソフトウェアがアップデートされた後でリブートするよう、H(e)NB1505に命令するのに使われるリブートコマンドを含む。ファームウェア/ソフトウェアアップデートの完了が成功した後で、転送完了が、SeGW1510に送られ得る(11)。或いは、TransferComplete RPCメソッドをH(e)NB1505から呼び出して、ファームウェア/ソフトウェアアップデートのプロシ

10

【0142】

プラットフォーム妥当性確認および管理(PVM)アーキテクチャにおいてSAVを用いるアーキテクチャおよび方法について本明細書に記載する。PVMは、デバイスを妥当性確認し管理するための体系的方法を提供し、デバイスは最初に、通信ネットワークに付属し、続いて、信頼できるコンピューティングからのセキュリティ技術に部分的に依拠して、デバイス完全性を監視しようとする。PVMは、1)ネットワーク接続が許可される前にデバイスを妥当性確認し、2)デバイス構成をOTA(無線経由で)管理し、3)コンポーネントロード/スタートにおけるRIMをチェックすることによって安全にスタートアップし、4)構成変更のために新規RIMをデバイスにインストールし、すなわちRIM摂取を行う。

20

【0143】

PVMでは、以下の用語が使われ得る。「検証(verification)」という用語は、安全なスタートアップ中のデバイスコンポーネントの内部検証に使うことができ、「妥当性確認(validation)」という用語は、外部エンティティによってデバイスをチェックするプロセス全体に対して使われる。したがって、「内部」対「外部」妥当性確認の導入が避けられる。検証が、暗号チェックまたはデータのマッチングの普通の意味で適用される場合は、混乱を生じないように明記する。

30

【0144】

PVMは、少なくともSeGW、PVE、およびDMSを使う。デバイス内のTrEは、デバイスの内側で妥当性確認に不可欠なタスクを実施し、概してTrEは、他のエンティティと通信する。デバイスの他のコンポーネント、例えば、この通信に必要とされるネットワークインタフェースは、必ずしもTrEの統合された一部ではないが、TrEがこうしたコンポーネントの完全性を評価して、エンドツーエンドのセキュリティを確実にすることは可能であるべきである。

【0145】

任務の厳密な区別には、各エンティティがそのコアタスクに制限されることが求められる。例えば、SeGWは、信頼できる(できない)デバイスとMNOのCNとの間の安全なインタフェースを構築する。このインタフェースは、MNOのCNのための障壁並びにネットワークアクセス制御および強化インスタンスとして作用する。このインタフェースは、このような障壁として作用するのに必要な、認証、デバイスとの通信の暗号化/復号、セキュリティアソシエーションおよびセッション確立を含む全セキュリティ関連機能も実施する。SeGWは、MNOのCNと、外部デバイスなどの外界との間の境界を構築するネットワークエンティティの例として使われ得る。SeGWの必要なく、PVM方法を用いてデバイス妥当性確認を実施することが可能でよい。こうすることは、TLS(トランスポートレイヤセキュリティ)など、安全にされた接続を用いる、DMSへのデバイス

40

50

の直接接続を含み得る。

【0146】

PVEに関しては、CN内の妥当性確認エンティティとして作用し、完全性の妥当性確認を実施する。PVEは、完全性検証データを受信し、報告された値が既知であり良好かどうかチェックする。PVEは、デバイス完全性についてのステートメントを、CN内の他のエンティティに対して発行する。

【0147】

DMSに関しては、ソフトウェアアップデート、構成変更、OTA管理および失敗モード修復を含む、デバイスコンポーネントの管理のための中心的エンティティとして作用する。DMSは、プラットフォーム妥当性確認に基づいてこの機能を始める際、H(e)MSの強化バージョンと同様である。

10

【0148】

上記エンティティに加え、PVMは、RIMマネージャ(RIMman)も含む。RIMmanは、妥当性確認における比較のための参照値の管理およびプロビジョニングを含む以下のタスクを実施する。RIMmanは、証明書、特に、外来RIM証明書の摂取、RIM証明書の検証、(オペレータ特有)RIM証明書の生成、および、例えば、撤回、時間制限および信頼関係による証明書妥当性のチェックも管理する。つまり、RIMマネージャは、一意のエンティティであり、妥当性確認データベース(V__DB)を管理することを認可されている。V__DBおよびRIMmanは、保護されたCNコンポーネントである。V__DBへの書き込みアクセスは、RIMmanのみに限られるので、PVEはV__DBに書き込むことができない。RIMmanは、PVMに必要な(SHO-CN)外部の信頼関係を管理するので、セキュリティに関して特に重要である。

20

【0149】

PVMは、デバイス構成の管理およびプロビジョニングを実施する構成ポリシーマネージャ(CPman)も含む。CPmanは、ポリシー、特に、例えば、TTP(信頼できるサードパーティ)からの外来構成およびポリシーの摂取、並びに(オペレータ特有)ターゲットデバイス構成およびポリシーの生成も管理する。つまり、CPmanは、一意のエンティティであり、構成ポリシーデータベースC__DBを管理することを認可されている。CPmanは、PVMに必要な(SHO-CN)外部の信頼関係を管理するので、セキュリティに関して特に重要である。

30

【0150】

図17A、17Bは、最小エンティティセット、その関係およびPVM用インタフェースの例を示す。AAA(認証、認可&アカウントिंग)サーバ並びにWTRU(ワイヤレス送受信ユニット)およびそのインタフェースなどの追加エンティティを、図示してある。

【0151】

図17AのPVMアーキテクチャまたはシステム1700は、TrE1710をもつデバイス1705を含む。WTRU1712(またはユーザエンティティ(UE))は、I-ueインタフェース1714を介してデバイス1705と通信することができる。デバイス1705は、I-hインタフェース1715を介してSeGW1720と通信する。概して、デバイス1705とSeGW1720との間のインタフェースI-h1715は、保護されなくてよく、真正性、完全性およびオプションで、機密性のための特殊措置が、安全なこのチャンネルに適用され得る。I-h1715は、デバイス1705とSeGW1720およびしたがってCNとの間のリンクを確立するのに使われ得る。例えば、SeGW1720は、インタフェースI-aaa1775を介してAAAサーバと通信し得る。オペレータは、インタフェースのセキュリティを確実にするための適切な措置を確立済みでよい。

40

【0152】

I-pveインタフェース1722は、SeGW1720によって、妥当性確認中にPVE1724に接触するのに使われ得る。PVE1724は、I-pveインタフェース

50

1722を使って、妥当性確認の出力結果をSeGW1720にシグナリングすることができる。Idmsインタフェース1730は、DMS1735とSeGW1720との間のデバイス構成関連通信に使われ得る。Ipdインタフェース1732は、PVE1724によって、DMS1735と、およびその反対に通信を行うのに使われ得る。このインタフェース、すなわちIpd1732は、デバイスソフトウェアアップデートおよび構成変更のためなど、デバイス管理プロシージャ中に使われ得る。

【0153】

インタフェースIv1726およびId1738は、それぞれ、PVE1720によって、V__DB1740からRIMを読み出すのに、また、DMS1735によって、許可された構成をC__DB1750から読み出すのに使われ得る。インタフェースI-r1728およびI-c1734は、V__DB1740中になくRIMのケースなどでは、PVE1720によって、RIMman1760と通信するのに、また、DMS1735によって、CPman1770と通信するのに使われ得る。RIMman1760およびCPman1770は、インタフェースI-rdb1762およびI-cdb1772を使って、それぞれ、データベースV__DB1740および構成ポリシーデータベースC__DB1750の妥当性確認を読み出し、書き込み、管理することができる。

【0154】

図17Bは、デバイス1705がDMS1735に直接接続し得るPVM1782を示す。デバイスがH(e)NBである場合、DMS1735は、本明細書において上で記載したように、H(e)MSになる。例えば、デバイス1705がSeGWとのセキュリティプロトコルを実施可能でないフォールバックモードの場合。この場合、DMS1735は、インタフェースIdms__d1784を介したデバイス1705用の第1の接触点として作用し、インタフェースI-pve1786およびIpd1788を介してPVE1724と通信して、妥当性確認を実施し、または少なくとも、どのコンポーネントが安全なスタートアップ中に失敗したかを知ることができる。DMS1735は、修復のためにこの情報に対して作用し得る。

【0155】

本明細書において述べたように、PVMは、妥当性確認のどのバージョンも使うこともできる。PVMと連動する半自律的妥当性確認(SAV)の実施形態について本明細書に記載する。半自律的妥当性確認(SAV)の高度妥当性確認方法に注目する。SAV用のこのソリューションの利点はさらに、CNが不良デバイスから完全に保護されることである。SAVの間、検疫が、SeGWによって有効に確立される。そのタスクに限られたデータのみを、SeGWとの安全な、またはSeGWによって確立された接続を介してのみ受信するので、デバイスからはPVEおよびDMSに対してどのような直接的脅威も課されない。SAVにおける妥当性確認プロセスは、デバイスとCN内のどのエンティティとの間の直接通信も求めない。SAVを用いた妥当性確認成功の後でのみ、CNへの接続が許可される。こうすることにより、証明された安全な状態にあるデバイスのみが、CNの内側のエンティティと通信し得ることが確実になる。

【0156】

図18A、18B、18Cは、PVMインフラストラクチャを用いるSAV妥当性確認方法の例の図を示す。PVMインフラストラクチャは、Tre1805、SeGW1807、PVE1809、DMS1811、V__DB1813およびC__DB1815を含む、本明細書に記載するエンティティを含む。相互認証(1820)に続いて、Tre1805は、Dev__ID、製造元、デバイス能力であって、サポートされるデータレートなどの通信能力、伝送電力レベル、シグナリング特徴および他の能力、Tre能力を含むが、それに限定されないデバイス能力などのデバイス情報、およびRotを含むプロパティと、ID、証明情報、製造元、ビルドバージョン、およびオプションでモデル、メーカー、シリアルナンバーを含むTre__informationと、1) デバイスの失敗した機能性のリスト、並びに/または2) PCR(プラットフォーム構成レジスタ)値、PCR値による署名などの検証バインディングまたは失敗したデバイス機能性のリスト、コンボ

ーメントに対するコンポーネントインジケータ (C I n d) の順序付きリスト C l i s t を含む検証データというデータの一部もしくは全部を収集することができ、コンポーネント用パラメータおよびタイムスタンプ (信頼できる、またはできない) を含む得る (1822)。T r E 1805からS e G W 1807への妥当性確認メッセージ／データは、上記日付を含む得る (1824)。

【0157】

S e G W 1807は、受信されたタイムスタンプを、ローカルタイムとチェック／比較して、変形を検出しなければならない (1826)。報告されたタイムスタンプがローカルタイムと合致しない場合、S e G Wは、報告されたタイムスタンプのプロパティに従って作用する。デバイスのタイムスタンプが、信頼できるタイムスタンプであり、変化を示す場合、S e G W 1807は、T r Eおよびその信頼できるタイムソースの再妥当性確認をトリガするべきである。信頼できないタイムスタンプのケースでは、S e G W 1807は、それ自体の信頼できるタイムスタンプをメッセージに追加する。デバイスが、信頼できるタイムスタンプを提供可能でない場合、S e G W 1807は、反射攻撃に対する保護として、信頼できるタイムスタンプを追加すればよい。

【0158】

このメッセージを受信すると、S e G W 1807は、T r Eからの署名の形の検証バインディングが存在するかどうかチェックすることができる (1828)。このチェックにより、検証データの真正性が確実にされる。S e G W 1807は次いで、P V Mトークン (T _ P V M) を作成し (1830)、送付前にT _ P V Mに対してタイムスタンプを印加して、フレッシュネスを確約し、非同期メッセージフローを防止する (1832)。

【0159】

S e G w 1807は、T _ P V MをP V E 1809にフォワードし (1834)、P V E 1809は、T r E情報を使ってV _ D B 1813を照会する (1836)。信用できない判定がP V E 1809に戻された (1838) 場合、P V Eは、T _ P V Mにタイムスタンプを印加し (1840)、S e G W 1807にフォワードする (1842)。S e G W 1807は、デバイス妥当性確認の拒否をT r E 1805に送る (1844)。

【0160】

信用できる判定がP V E 1809に戻された (1846) 場合、P V Eは、D e v _ I Dを使ってC _ D Bを照会し (1848)、C _ D Bは、構成ポリシー (1850) をP V E 1809に戻す。P V E 1809は、ポリシー構成を評価する (1852)。

【0161】

P V E 1809が、構成は信用できない (1854) と判定した場合、P V E 1809は、T _ P V Mを修正し、タイムスタンプを印加する (1856)。P V E 1809は次いで、T _ P V MをS e G W 1807にフォワードし (1858)、S e G W 1807は、デバイス妥当性確認の拒否をT r E 1805に送る (1860)。

【0162】

P V E 1809が、構成は信用できると判定し、構成を許可した (1862) 場合、P V E 1809は、V _ D B 1813からC l i s tまたはC _ L i s t中の全エントリに対するR I Mを取り出す (1864)。P V E 1809は、R I Mから正しい検証データを算出し直し (1866)、算出された検証データを、報告された検証データと比較する (1868)。S A Vのケースでは、R I Mから算出された検証データは、失敗した機能性の「空リスト」の形になる。P V E 1809は次いで、T _ P V Mを修正し、タイムスタンプを印加する (1870)。P V E 1809は次いで、T _ P V MをS e G W 1807にフォワードする (1872)。S e G W 1807は、P V E妥当性確認結果に関してT _ P V Mを検査する (またはT _ P V Mから抽出する) (1874)。S e G W 1807は、デバイス妥当性確認の拒否または許可をT r E 1805に送る (1876)。P V E妥当性確認結果が否定である場合、T r E 1805は、リブートを実施し、再妥当性確認を行う (1890)。

【0163】

オプションで、PVE1809が、算出された検証データを、報告された検証データと比較した(1868)後、PVE1809は、失敗したコンポーネントのリストをDMS1811に送ることができる(1878)。失敗したコンポーネントのリストが空でない場合、DMS1811は、ソフトウェアまたはファームウェアのアップデートを適用することができる(1880)、適用できる場合、OTAアップデートを準備する(1882)。DMS1811は、アップデートのためのRIMがV_DB1813中に存在することも確実にする(1884)。DMS1811は、再妥当性確認の指示とともにT_PVMをSeGW1807に(1886)、また、再妥当性確認トリガをTRE1805に(1888)送る。TRE1805は、リポートを実施し、再妥当性確認を行う(1890)。

10

【0164】

図18A、18B、18Cにおける処理に関する詳細について本明細書に記載する。プラットフォーム妥当性確認を実施するために、TREは、以下のデータを収集し、SeGWに伝達する。すなわち、Dev_ID、製造元、TRE能力およびROTを含むプロパティなどのデバイス情報と、ID、証明情報、製造元、ビルドバージョン、およびオプションでモデル、メーカー、シリアルナンバーを含むTRE_informationと、完全性検証データ(IVD)(IVDの一例は、署名されたPCR(プラットフォーム構成レジスタ)値でよく、別の例は単に、その完全性がデバイスにローカルな完全性チェックプロセスによってチェック済みであり、さらにこのようなデバイスにローカルな完全性チェックに失敗したとして評価済みであるコンポーネントまたは機能性のリストでよい)と、PCR値による署名などの検証バインディングと、コンポーネントClistに対するコンポーネントインジケータ(CInd)の順序付きリストであるとともにコンポーネント用パラメータを含み得るClistとである。コンポーネントのリストは、例えば、RIM証明書、すなわちRIMcsをポイントすることによって、妥当性確認用RIMを識別するのに役立つ。コンポーネントおよびそのパラメータに対するインジケータの順序付きリストは、索引、component_indicator CInd、component_parametersというデータフィールドなどのエントリを含むことになる。CIndは、コンポーネントへの参照を与え、URN形式でよい(例えば、URN:/vendor.path.to/component/certificate)。オプションで、タイムスタンプ(信頼できるタイムスタンプでも、概して必ずしも信頼できるわけではない通常のタイムスタンプでもよい)がある。

20

30

【0165】

デバイスのケースでは、妥当性確認メッセージは、ID、証明情報、製造元、モデル、バージョン、メーカー、シリアルナンバー、ROTを含むTRE能力およびプロパティ、デバイスのセキュリティポリシー、完全性検査および事後検査コンポーネントローディングの複数ステッププロセスの異なる段階で完全性チェックされるモジュール、HWビルドバージョン番号、並びにオプションでSWビルドバージョン番号および完全性測定データなどのデバイス情報をさらに含み得る。

【0166】

妥当性確認のためにRIMを使用することは、好ましいがオプションのSAVのための方法である。ここではベースケースとして使われ、他の選択肢はこのケースからはずれ、逸脱する。例えば、RIMから検証データを算出し直さない妥当性確認があり、実施用PVMを完全にRIMなしで行う可能性さえもある。

40

【0167】

検証バインディングは、デバイスの完全性を伴うもの以外の手段によって、例えば、安全なチャネルの存在および使用によって妥当性確認メッセージが認証にバインドされる場合はオプションでよい。

【0168】

SeGWは、受信されたタイムスタンプを、ローカルタイムとチェック/比較して、変形を検出することができる。報告されたタイムスタンプが、ローカルタイムと合致しない

50

場合、S e G Wは、報告されたタイムスタンプのプロパティに従って作用する。デバイスのタイムスタンプが、信頼できるタイムスタンプであり、変化を示す場合、S e G Wは、T r Eおよびその信頼できるタイムソースの再妥当性確認をトリガすることができる。信頼できないタイムスタンプのケースでは、S e G Wは、それ自体のタイムスタンプをメッセージに追加する。

【0169】

T r E__i n f oはオプションでよい。D e v__I Dは、T r E__i n f oへの参照を与え得る。全M N Oが全T r Eを、およびしたがって全T r E__i n f oデータを知るわけではないので、このようなマッピングは、所与の任意のD e v__I Dに関するT r E__i n f oを取得するためにM N Oによって照会され得るデータベースによって与えられ得る。T r E__i n f oは、T r E__c e r t i f i c a t e中にあり得る。T r E__c e r t i f i c a t eは、T r EまたはT T Pのベンダ、例えば、独B S Iによって署名されるべきである。

10

【0170】

コンポーネントに対するインジケータ（C I n d）としてのU R Nの使用は、コンポーネントおよびR I MまたはR I M証明書を取り出すことができる場所のこの一意の識別を同時に許可するので、有利である。

【0171】

S e G Wは、ローリングトークンとして使うことができるとともに通信中にエンティティからエンティティに渡されるP V Mトークン（T__P V M）を作成する。すべてのエンティティは、送付前にトークンにタイムスタンプを押して、フレッシュネスを確約し、非同期メッセージフローを防止する。トークンに対するタイムスタンプは、トークンの状態に従う方法を提供するのに使われ得る。トークンは、C N内でエンティティからエンティティに何巡も移動することができ、したがって、エンティティによって追跡することができる。オプションで、エンティティI Dが、タイムスタンプされたデータの連鎖に組み込まれ得る。

20

【0172】

T__P V Mは、D e v__I Dを含み得る。オリジナルタイムスタンプが存在せず、または信頼されない場合、T__P V Mは、S e G Wによって発行される新規タイムスタンプを含んでもよい。そうでない場合、T__P V Mは、妥当性確認メッセージからのオリジナルタイムスタンプを含み得る。

30

【0173】

タイムスタンプは、反射攻撃に対する保護に使われ得る。タイムスタンプは、ノンスまたは単調に増加するカウンタと組み合わせることも、それで置き換えることもできる。タイムスタンプは、妥当性確認データのフレッシュネスを評価するのに使うこともできる。両方の目的を組み合わせることが有利であり、タイムスタンプによって提供され得る。

【0174】

第1の変形体において、D M Sによる以降のデバイス管理のために、T__P V Mは、D M SとT r E、例えば、T L S証明書との間の安全なトンネルを構築する通信秘密を含み得る。

40

【0175】

S e G Wは、全アクティブT__P V Mを含むトークンデータベースT__D Bを維持する。

【0176】

S e G Wは、妥当性確認データ、T r E__i n f o、およびC l i s tというデータを妥当性確認メッセージから抽出する。このデータをトークンT__P V Mと一緒に送る前に、S e G Wは、T__P V Mにタイムスタンプを押し、P V Eにフォワードする。S e G Wは、妥当性確認メッセージおよびその一部の形式をチェックして、不正形式のデータ攻撃からの脅威を軽減させることができる。そうしないと、P V Eでのこのデータの純粋な検査が、システムエラーまたは失敗につながるように、攻撃者が、危害を受けたT r Eの妥

50

当性確認メッセージ中のデータを修正しようとする可能性がある。

【0177】

PVEは、デバイスの妥当性を決定するエンティティである。つまり、ポリシーシステムの言葉では、ポリシー決定点(PDP)である。任務の厳密な区別という手法の下では、PVEはPVMシステム内の唯一のPDPである。PDPは、SeGWおよびDMSに依拠して、ポリシー施行点(PEP)として作用するなどのポリシーを施行する。PVMは、その概要において、どのようにポリシーが生成されるか、および、どこからPVEがポリシーを得るかなど、どこに格納／管理されるかという疑問を問わないままである。後で説明するより詳細な変形体および付随方法の一部では(特定のパラメータに関する妥当性確認および最低限の妥当性確認では)、ポリシー条件およびアクションの幾つかの例が挙げられる。概して、妥当性確認ポリシーの決定は、単一のコンポーネントの妥当性だけではなく、Clistに含まれる他のデータにも基づき得る。特に、許可されるパラメータ(範囲)、およびロードの順序(Clistが順序づけられる)が評価され得る。

10

【0178】

PVEによって実行される妥当性確認プロセス中に起こり得る失敗条件の幾つかの根本的クラスがある。例えば、失敗条件F1は、「TRE無効」シナリオを示す。認証されたそのDev_IDおよび配布されたTRE_infoによって、PVEは、デバイスおよび／またはそのTREを、信用できないものと識別する。注：TREが無効であり得るかどうか判定するのに用いられ得る情報は、SAV妥当性確認メッセージ自体にのせて搬送することができ、または他のメッセージもしくは他の手段から推定することができる。その基本的な形において、SAV妥当性確認メッセージの存在は、TRE自体が有効でなければならないことを暗黙的に示し得る。F1がどのように検出され得るかについての詳細は、本明細書において完全に説明されているものとして、参照によって組み込まれている、同時に出版した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に論じられている。

20

【0179】

別の例は、「IVD検証失敗」に関する3つのシナリオを示す失敗条件F2である。シナリオF2aは、完全性測定／検証データ不一致を示す。F2aは、デバイスの安全なスタートアッププロセスの失敗、並びに／またはデバイス上での偽および／もしくは失効したRIMおよび／もしくはRIM証明書の存在を示し、これにより次いで、無効コンポーネントがスタートされる。シナリオF2bは、RIM欠如を示し、すなわち、コンポーネント用RIMが欠如しており、どこか他の所から取り出される必要がある。シナリオF2cは、失効したRIM証明書を示す。

30

【0180】

失敗条件F3は、「Clistポリシー失敗」に関する2つのシナリオを示す。シナリオF3aに対して、単一のコンポーネントが有効であるが、構成は、例えば、ロード順序、または望まれないコンポーネント、またはパラメータに対するポリシーに失敗する。シナリオF3bは、Clistの「既知の良好値」が利用できないように、構成が未知であることを示す。

【0181】

失敗条件クラスF2の検出および取扱い方法について本明細書に記載する。失敗条件F2に対して、PVEは、受信されたClistにある全コンポーネント用のV__DBからRIMを取り出す。妥当性確認データベースV__DBは、認証されたRIMのみを格納する。対応するRIM証明書は、V__DBに安全に格納されなければならない。

40

【0182】

IVDが、本明細書に記載した狭義のSAVプロシージャに記載されるように、「ローカル完全性検査に失敗した、デバイスのコンポーネントに対応する、デバイスのコンポーネント」の単純なリストの形である場合、IVD_refは、単にNULLリストの形になる。つまり、IVD_refは、この場合、失敗した機能性の期待されるリストに過ぎないはずであり、このリストは、すべてのコンポーネントがデバイスにローカルな完全性検査

50

を通ったことを期待される場合はNULLテーブルであるべきである。

【0183】

I V D _ r e f が受信された I V D と合致しない場合、デバイス上での安全なスタートアッププロセスが危害を受けており、または誤った R I M がデバイスに格納されており、したがって無効コンポーネントが安全なスタートアッププロセス中にロードされている。

【0184】

F 2 a ポリシーに依存して、F 2 a 失敗が検出されると、幾つかの選択肢が該当し得る。1つの選択肢では、拒絶である。P V E は、妥当性確認の出力結果を S e G W にシグナリングする。S e G W は次いで、ネットワークアクセスを拒否しても、デバイスを検疫ネットワークに入れてもよい。第2の選択肢はアップデートである。検証データ失敗を示す妥当性確認結果 (T _ P V M) を受信した後、D M S は、管理プロセスをスタートして、妥当性確認に失敗したコンポーネントを置き換える。このような修復プロセスの詳細は、本明細書において完全に説明されているものとして、参照によって組み込まれている、同時に出版した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に論じられている。

【0185】

どのポリシー失敗条件も満たされない場合、デバイスは有効である。P V E は、このことを S e G W にシグナリングし、S e G W は次いで、C N への接続を許可する。

【0186】

R I M が欠如している失敗条件 F 2 b の場合、これは、R I M が V _ D B 中にないか、またはデバイスにない（その結果、この場合、デバイスは、デバイスにローカルな完全性検査プロシーダを実施することができなくなる）ので、起こり得る。F 2 がどのように検出され取り扱われ得るかについての詳細は、本明細書において完全に説明されているものとして、参照によって組み込まれている、同時に出版した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に論じられている。

【0187】

失敗条件クラス F 3 の検出および取扱い方法について本明細書に記載する。F 3 失敗条件は、単一のコンポーネントが有効であるがコンポーネントの構成がポリシーに失敗した（例えば、ロード順不一致）場合、または構成が未知である、すなわち、C l i s t の「既知の良好な値」が入手できない場合に起こる。このような失敗条件がどのように起こり得るか、およびこのような失敗条件がどのように取り扱われ得るかについての詳細は、本明細書において完全に説明されているものとして、参照によって組み込まれている、同時に出版した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に論じられている。

【0188】

図19は、H (e) N B を含む L T E (ロングタームエボリューション) ワイヤレス通信システム／アクセスネットワーク1900とともに使われ得る E - U T R A N (進化的ユニバーサル地上無線アクセスネットワーク) 1905を示す。E - U T R A N 1905は、W T R U 1910、および幾つかの e N B (evolved Node-B) 1920を含む。W T R U 1910は、e N B 1920と通信する。e N B 1920は、X 2 インタフェースを使って互いにインタフェースをとる。e N B 1920はそれぞれ、S 1 インタフェースを介して、M M E (移動管理エンティティ) / S - G W (サービングゲートウェイ) 1930とインタフェースをとる。単一の W T R U 1910 および 3 つの e N B 1920 を図19に示してあるが、ワイヤレスおよびワイヤードデバイスのどの組合せも、ワイヤレス通信システムアクセスネットワーク1900に含まれ得ることが明らかであろう。

【0189】

図20は、W T R U 1910、e N B 1920、および M M E / S - G W 1930 を含む L T E ワイヤレス通信システム2000の例示的ブロック図である。図20に示すように、W T R U 1910、e N B 1920 および M M E / S - G W 1930 は、自律的および

び半自律的妥当性確認を用いるH (e) NB完全性検証および妥当性確認の方法を実施するように構成される。

【0190】

典型的なWTRUにおいて見られ得るコンポーネントに加え、WTRU 1910は、オプションのリンクされたメモリ2022を有するプロセッサ2016、少なくとも1つのトランシーバ2014、オプションのバッテリー2020、およびアンテナ2018を含む。プロセッサ2016は、自律的および半自律的妥当性確認を用いるH (e) NB完全性検証および妥当性確認の方法を実施するように構成される。トランシーバ2014は、プロセッサ2016およびアンテナ2018と通信して、ワイヤレス通信の送受信を容易にする。WTRU 1910内でバッテリー2020が使われるケースでは、バッテリー2020は、トランシーバ2014およびプロセッサ2016に電力を供給する。

10

【0191】

典型的なeNB (H (e) NBを含む)において見られ得るコンポーネントに加え、eNB 1920は、オプションのリンクされたメモリ2015を有するプロセッサ2017、トランシーバ2019、およびアンテナ2021を含む。プロセッサ2017は、自律的および半自律的妥当性確認を用いるH (e) NB完全性検証および妥当性確認の方法を実施するように構成される。トランシーバ2019は、プロセッサ2017およびアンテナ2021と通信して、ワイヤレス通信の送受信を容易にする。eNB 1920は、オプションのリンクされたメモリ2034を有するプロセッサ2033を含むMME / S-GW (移動管理エンティティ / サービングゲートウェイ) 1930に接続される。

20

【0192】

S e GWおよびP V Eは、図19、20には示していないが、典型的なS e GWおよびP V Eにおいて見ることができるコンポーネントに加え、オプションのリンクされたメモリ、トランシーバ (複数可)、アンテナ (複数可)、および通信ポートを有するプロセッサを含み得る。プロセッサは、プラットフォーム妥当性確認および管理機能を実施して、P V M手順を実装するように構成される。トランシーバおよび通信ポートは、必要に応じて、プロセッサおよびアンテナと通信して、通信内容の送信および受信を容易にする。

【0193】

実施形態

1. H (e) NB (home evolved Node B) の完全性検証を実施する方法であって、コンポーネントのローディングに先立って、コンポーネントに関する完全性メトリックを測定することを含む方法。

30

【0194】

2. 実施形態1の方法において、信頼できる参照値 (TRV) を認証することをさらに含む方法。

【0195】

3. 上記実施形態のいずれかに記載の方法において、測定された完全性メトリックをTRVと比較することをさらに含む方法。

【0196】

4. 上記実施形態のいずれかに記載の方法において、完全性検証結果に依存して、通常コードまたはフォールバックコードの一方で、H (e) NBをスタートすることをさらに含む方法。

40

【0197】

5. 上記実施形態のいずれかに記載の方法において、ソフトウェアモジュールと、参照完全性メトリック、並びにH (e) NBおよびプラットフォーム妥当性確認エンティティ (P V E) の少なくとも一方に対する重大度の少なくとも1つを含む、関連付けられた属性のリストとを提供することをさらに含む方法。

【0198】

6. 上記実施形態のいずれかに記載の方法において、デバイス構成データシートは、ソフトウェアモジュールおよび関連付けられた属性のリストを含み、H (e) NBおよびP

50

プラットフォーム妥当性確認エンティティ（PVE）の少なくとも一方に与えられる方法。

【0199】

7. 上記実施形態のいずれかに記載の方法において、関連付けられた属性は、コンポーネントおよび機能性に関して、ソフトウェアモジュールのマッピングを可能にする方法。

【0200】

8. 上記実施形態のいずれかに記載の方法において、デバイス構成データシートと、ソフトウェアモジュールおよび関連付けられた属性のリストとの少なくとも一方は、H(e)NBおよびプラットフォーム妥当性確認エンティティ（PVE）の少なくとも一方に格納される方法。

【0201】

9. 上記実施形態のいずれかに記載の方法において、PVEがそれに基づいてアクションを判定し得るモジュール識別子を少なくとも含む完全性チェック失敗メッセージを送ることをさらに含む方法。

【0202】

10. 上記実施形態のいずれかに記載の方法において、完全性検証失敗に対する重大度分類に基づいて所定のアクションを実施することをさらに含む方法。

【0203】

11. 上記実施形態のいずれかに記載の方法において、所定のアクションは、非常メッセージの送付、コードアップデートの開始、修復の開始、および失敗した機能性のリストの報告の少なくとも1つを含む方法。

【0204】

12. 上記実施形態のいずれかに記載の方法において、ソフトウェアモジュールおよび関連付けられた属性のリストは、コンポーネント特有の情報要素、モジュール特有の情報要素および機能要素の少なくとも1つを含む方法。

【0205】

13. 上記実施形態のいずれかに記載の方法において、コンポーネント特有の情報要素は、コンポーネント説明、コンポーネント識別（ID）および信頼できる参照値（TRV）の少なくとも1つを含む方法。

【0206】

14. 上記実施形態のいずれかに記載の方法において、モジュール特有の情報要素は、モジュール説明、モジュール識別（ID）、機能説明、機能ID、コンポーネントID、リリースバージョンおよび重大度の少なくとも1つを含む方法。

【0207】

15. 上記実施形態のいずれかに記載の方法において、モジュールは、完全性検証中に少なくとも一度調べられる方法。

【0208】

16. 上記実施形態のいずれかに記載の方法において、モジュールは、ただ1つのコンポーネント中に現れる方法。

【0209】

17. 上記実施形態のいずれかに記載の方法において、モジュールは、2つの機能の間で共有される方法。

【0210】

18. 上記実施形態のいずれかに記載の方法において、各モジュールは、関連付けられた機能性をもつ方法。

【0211】

19. 上記実施形態のいずれかに記載の方法において、モジュールグループは、同じコンポーネントに関連付けられ、同じコンポーネント識別子（ID）を共有し、同じコンポーネントとの完全性をまとめて検証される方法。

【0212】

20. 上記実施形態のいずれかに記載の方法において、1つのコンポーネント識別子（

10

20

30

40

50

I D)をもつモジュールは、異なる機能性識別子 (I D) で分類される方法。

【0213】

21. 上記実施形態のいずれかに記載の方法において、モジュールは、機能性および完全性チェック単位に基づいて分類される方法。

【0214】

22. 上記実施形態のいずれかに記載の方法において、同じコンポーネント識別子のモジュールは、1つの信頼できる参照値 (T R V) をもち、信頼できる参照値が失敗するという条件で、失敗したコンポーネント識別子の全モジュールは、失敗した機能性のリストを判定するのに使われる方法。

【0215】

23. H (e) N B (h o m e e v o l v e d N o d e B) の妥当性確認を実施する方法であって、デバイス完全性チェック失敗の結果、上記 H (e) N B をフォールバックコードでスタートすることを含む方法。

【0216】

24. 上記実施形態23の方法において、非常メッセージを送ることをさらに含む方法。

【0217】

25. 上記実施形態23～24のいずれかに記載の方法において、修復情報を取り出すダウンリンクメッセージを受信することをさらに含む方法。

【0218】

26. 上記実施形態23～25のいずれかに記載の方法において、ダウンリンクメッセージに応答して修復情報をダウンロードすることをさらに含む方法。

【0219】

27. 上記実施形態23～26のいずれかに記載の方法において、インストールされた修復情報に基づいて H (e) N B をリスタートすることをさらに含む方法。

【0220】

28. 上記実施形態23～27のいずれかに記載の方法において、失敗情報をアップロードして、修復情報の準備を許すことをさらに含む方法。

【0221】

29. 上記実施形態23～28のいずれかに記載の方法において、非常メッセージは、製造元識別、信頼できる環境識別、H (e) N B 識別、および失敗コードの少なくとも1つを含む方法。

【0222】

30. 上記実施形態23～29のいずれかに記載の方法において、重大度測度は、デバイス完全性チェック失敗の影響を指定する方法。

【0223】

31. 上記実施形態23～30のいずれかに記載の方法において、デバイス完全性チェックは、ローカルに実施される方法。

【0224】

32. 上記実施形態23～31のいずれかに記載の方法において、失敗情報は、H (e) N B 管理システム (H (e) M S) またはプラットフォーム妥当性確認エンティティ (P V E) の一方に送られる方法。

【0225】

33. 上記実施形態23～32のいずれかに記載の方法において、H (e) N B は、S S L / T L S (セキュアソケットレイヤ/トランスポートレイヤセキュリティ) を使って、非常メッセージを送る方法。

【0226】

34. 上記実施形態23～33のいずれかに記載の方法において、H (e) N B は、デフォルトの H (e) M S U R L (ユニフォームリソースロケータ) で構成される方法。

【0227】

10

20

30

40

50

35. 上記実施形態23～34のいずれかに記載の方法において、デバイス構成データシートは、デバイスの安全なメモリ内部に維持され、認可された当事者によってアクセスされる方法。

【0228】

36. 上記実施形態23～35のいずれかに記載の方法において、H(e)NBは、デバイス構成データシートが満了すると、アップデートプロセスを開始して、修復サーバからデータをプルする方法。

【0229】

37. 上記実施形態23～36のいずれかに記載の方法において、H(e)NBは、予め指定されたコンポーネントのデバイス完全性チェックを実施する方法。

10

【0230】

38. 上記実施形態23～37のいずれかに記載の方法において、PVEからH(e)NBアクションを受信することをさらに含む方法。

【0231】

39. H(e)NB(home evolved Node B)の妥当性確認を実施する方法であって、IKE(インターネット鍵交換)セキュリティアソシエーションを確立することを含む方法。

【0232】

40. 実施形態1の方法において、デバイス完全性チェック結果の相互認証および指示のための証明書を、IKE__AUTH要求に入れて送ることをさらに含む方法。

20

【0233】

41. 上記実施形態39～40のいずれかに記載の方法において、認証およびデバイス完全性の妥当性確認の結果の指示を受信することをさらに含む方法。

【0234】

42. 上記実施形態39～41のいずれかに記載の方法において、デバイス完全性チェック結果の評価に基づくアクションを受信することをさらに含む方法。

【0235】

43. 上記実施形態39～42のいずれかに記載の方法において、デバイス完全性チェック結果は、失敗した機能性のリストを含む方法。

【0236】

30

44. 上記実施形態39～43のいずれかに記載の方法において、受信されたアクションは、修復を呼び出す方法。

【0237】

45. 上記実施形態39～44のいずれかに記載の方法において、H(e)NB内でのデバイス完全性チェック結果は、検疫され、完全アクセスを入手し、部分アクセスを入手し、または修復のための担当者介入を入手する方法。

【0238】

46. 上記実施形態39～45のいずれかに記載の方法において、修復を示すアクションに応答して非常メッセージを送ることをさらに含む方法。

【0239】

40

47. 上記実施形態39～46のいずれかに記載の方法において、修復情報を取り出すダウンリンクメッセージを受信することをさらに含む方法。

【0240】

48. 上記実施形態39～47のいずれかに記載の方法において、ダウンリンクメッセージに応答して修復情報をダウンロードすることをさらに含む方法。

【0241】

49. 上記実施形態39～48のいずれかに記載の方法において、インストールされた修復情報に基づいてH(e)NBをリスタートすることをさらに含む方法。

【0242】

50. 上記実施形態39～49のいずれかに記載の方法において、失敗情報をアップロ

50

ードして、修復情報の準備を許す方法。

【0243】

51. 上記実施形態39～50のいずれかに記載の方法において、失敗情報は、失敗した機能性のリストを含む方法。

【0244】

52. 上記実施形態39～51のいずれかに記載の方法において、失敗情報は、H(e)NB管理システム(H(e)MS)またはプラットフォーム妥当性確認エンティティ(PVE)の一方に送られる方法。

【0245】

53. 上記実施形態39～52のいずれかに記載の方法において、失敗情報は、チェックされた機能性のリストを含む方法。

10

【0246】

54. 上記実施形態39～53のいずれかに記載の方法において、失敗情報は、チェックされていない機能性のリストを含む方法。

【0247】

55. 上記実施形態39～54のいずれかに記載の方法において、妥当性確認および認証のバインドは、IKEセッションによって与えられる方法。

【0248】

56. 上記実施形態39～55のいずれかに記載の方法において、妥当性確認および認証のバインドは、デバイス完全性検査が成功するという条件で先行する認証プロセスによって与えられる方法。

20

【0249】

57. デバイス妥当性確認をバインドする方法であって、信頼できる環境(TrE)を認証プロセスにバインドすることを含む方法。

【0250】

58. 実施形態57の方法において、認証プロセスは、EAP-AKA(Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement)プロセスである方法。

【0251】

59. 実施形態57～58のいずれか1つに記載の方法において、プロセスはAKA資格を妥当性確認する方法。

30

【0252】

60. 実施形態57～59のいずれか1つに記載の方法において、AKA資格はTrEに含まれる方法。

【0253】

61. 実施形態57～60のいずれか1つに記載の方法において、妥当性確認済みデバイスとEAP-AKAベース認証をバインドすることをさらに含む方法。

【0254】

62. 実施形態57～61のいずれか1つに記載の方法において、EAP-AKA認証は、AKA資格を保持するTrEを、EAP-AKAベース認証のプロセスにバインドすることを含む方法。

40

【0255】

63. 実施形態57～62のいずれか1つに記載の方法において、HeNB(enhanced home node B)へのAKA資格を保持するTrEの論理バインドを実施することをさらに含む方法。

【0256】

64. 実施形態57～63のいずれか1つに記載の方法において、デバイスプラットフォームの完全性が妥当性確認される方法。

【0257】

50

65. 実施形態57～64のいずれか1つに記載の方法において、HeNBへの、AKA資格を保持するTrEの物理的バインドを実施することをさらに含む方法。

【0258】

66. 実施形態57～65のいずれか1つに記載の方法において、ハードウェアおよびソフトウェアに対する実際の完全性の妥当性確認は、HeNBに安全に組み込まれたハードウェアセキュリティコンポーネントによって実施される方法。

【0259】

67. 実施形態57～66のいずれか1つに記載の方法において、EAP-AKA認証に適した資格および物理的にバインドされたTrEに格納された関連アプリケーションは、ホスティングデバイスへの取外し可能ハードウェアコンポーネントのバインドを妥当性確認するように構成される方法。

10

【0260】

68. 実施形態57～67のいずれか1つに記載の方法において、AKA資格を保持するTrEおよびHeNBはさらにバインドされる方法。

【0261】

69. 実施形態57～68のいずれか1つに記載の方法において、TrEのみがデータを復号することができるように、デバイス妥当性確認に使われるAKA資格を計算するのに必要とされるデータをHeNBが暗号化することをさらに含む方法。

【0262】

70. 実施形態57～69のいずれか1つに記載の方法において、HeNB暗号化データを復号するのに必要とされる鍵をTrEが安全に格納することをさらに含む方法。

20

【0263】

71. 実施形態57～70のいずれか1つに記載の方法において、共通セキュリティプロトコルの同じセッション中のデバイス妥当性確認およびデバイス認証についての情報を組み合わせて、さらなるバインディングを取得することをさらに含む方法。

【0264】

72. 実施形態57～71のいずれか1つに記載の方法において、共通セキュリティプロトコルは、IKEv2（インターネット鍵交換バージョン2）である方法。

【0265】

73. 実施形態57～72のいずれか1つに記載の方法において、デバイス妥当性確認は、HeNBとネットワークエンティティ間の対話およびメッセージ交換を含む方法。

30

【0266】

74. 実施形態57～73のいずれか1つに記載の方法において、HeNBはTrEを含む方法。

【0267】

75. 実施形態57～74のいずれか1つに記載の方法において、HeNBの妥当性確認をネットワークエンティティが実施することをさらに含む方法。

【0268】

76. 実施形態57～75のいずれか1つに記載の方法において、HeNBと妥当性確認を実施するネットワークエンティティとの間のシグナリングをセキュリティゲートウェイが伝えることをさらに含む方法。

40

【0269】

77. 実施形態57～76のいずれか1つに記載の方法において、デバイス妥当性確認を証明書ベースの認証にバインドすることをさらに含む方法。

【0270】

78. 実施形態57～77のいずれか1つに記載の方法において、バインドすることは、HeNBのTrEを証明書ベースのデバイス妥当性確認のプロシージャに物理的にバインドすることを含む方法。

【0271】

79. 実施形態57～78のいずれか1つに記載の方法において、バインドすることは

50

、H e N BのT r Eを証明書ベースのデバイス妥当性確認のプロシージャに論理的にバインドすることを含む方法。

【0272】

80. 実施形態57～79のいずれか1つに記載の方法において、証明書資格を保持するT r EとH e N Bはさらにバインドされる方法。

【0273】

81. 実施形態57～80のいずれか1つに記載の方法において、暗号鍵を使ってデバイス妥当性確認に使われる証明書資格を計算するのに必要とされるデータをH e N Bが暗号化すること、およびT r Eが安全に保持する鍵を使ってT r Eの内側の暗号化データをT r Eが復号することをさらに含む方法。

10

【0274】

82. 実施形態57～81のいずれか1つに記載の方法において、共通プロトコルセッションの同じまたは連続するセッションを両方のプロシージャに使わせることによって、証明書ベースの認証セッションをH e N B妥当性確認のためのプロシージャにバインドすることをさらに含む方法。

【0275】

83. 実施形態57～82のいずれか1つに記載の方法において、デバイス妥当性確認は、H e N Bと、ネットワークがH e N Bのデバイス完全性の妥当性確認を実施することを可能にするネットワークエンティティとの間の、共通プロトコルセッションによる対話を含む方法。

20

【0276】

84. 実施形態57～83のいずれか1つに記載の方法において、バインドされるH e N Bのデバイス妥当性確認をE A P - A K Aベースのクライアント認証にバインドすることをさらに含む方法。

【0277】

85. 実施形態57～84のいずれか1つに記載の方法において、T r EとH e N Bの残りとの間のメッセージ交換のための暗号鍵および資格を使ってT r EをH e N Bにバインドすることをさらに含む方法。

【0278】

86. 実施形態57～85のいずれか1つに記載の方法において、T r EとH e N Bの残りとの間のメッセージ交換は、デバイス妥当性確認に関連したメッセージ交換を含む方法。

30

【0279】

87. 実施形態57～86のいずれか1つに記載の方法において、鍵および資格は、T r Eの内側で保護される方法。

【0280】

88. 実施形態57～87のいずれか1つに記載の方法において、共通セキュリティプロトコルの同じまたは連続するセッション中に、デバイス妥当性確認およびE A P - A K Aベースのクライアント認証の指定された一部をH e N BおよびT r Eが実施することをさらに含む方法。

40

【0281】

89. 実施形態57～88のいずれか1つに記載の方法において、H e N Bのデバイス妥当性確認を証明書ベースのクライアント認証にバインドすることをさらに含む方法。

【0282】

90. 実施形態57～89のいずれか1つに記載の方法において、T r Eは、鍵ペアを含む方法。

【0283】

91. 実施形態57～90のいずれか1つに記載の方法において、鍵ペアは、私有部および公開部を含む方法。

【0284】

50

92. 実施形態57～91のいずれか1つに記載の方法において、私有部は、T r Eの内側に安全に格納される方法。

【0285】

93. 実施形態57～92のいずれか1つに記載の方法において、公開部は、H e N Bに対して使用可能にされる方法。

【0286】

94. 実施形態57～93のいずれか1つに記載の方法において、H e N Bの製造元が、鍵ペアを生成すること、およびH e N Bに対して公開鍵を利用可能にするのに必要とされる証明書を与えることをさらに含む方法。

【0287】

95. 実施形態57～94のいずれか1つに記載の方法において、E A P－A K A ベース認証における暗号手段によって、妥当性確認および認証のバインドを作成することをさらに含む方法。

【0288】

96. 実施形態57～95のいずれか1つに記載の方法において、H e N Bが、証明書からの公開鍵で応答を暗号化すること、および暗号化データをT r Eにフォワードすることをさらに含む方法。

【0289】

97. 実施形態57～96のいずれか1つに記載の方法において、応答はI K E __ A U T H 応答である方法。

【0290】

98. 実施形態57～97のいずれか1つに記載の方法において、T r Eが、次いで、データを復号すること、並びにA A A（認証、認可およびアカウントティング）サーバに対してH e N Bを認証するのに必要とされるE A P－A K A 応答（R E S）パラメータを計算することをさらに含む方法。

【0291】

99. 実施形態57～98のいずれか1つに記載の方法において、H e N Bが、公開鍵を使って、T r EにおけるA U T H パラメータを計算するのに必要とされるデータを暗号化することをさらに含む方法。

【0292】

100. 実施形態57～99のいずれか1つに記載の方法において、T r Eが、データを復号すること、およびS e G W に対するH e N Bを認証するのに必要なA U T H パラメータを計算することをさらに含む方法。

【0293】

101. 実施形態57～100のいずれか1つに記載の方法において、デバイス完全性とデバイスI D を暗号によってバインドすることをさらに含む方法。

【0294】

102. 実施形態57～101のいずれか1つに記載の方法において、デバイス完全性とデバイスI D を暗号によってバインドすることは、T r E およびH e N B によって実施される方法。

【0295】

103. 実施形態57～102のいずれか1つに記載の方法において、T r E およびH e N B は、それぞれの公開鍵ペアを装備する方法。

【0296】

104. 実施形態57～103のいずれか1つに記載の方法において、T r E およびH e N B は、それぞれの対称共有鍵を装備する方法。

【0297】

105. 実施形態57～104のいずれか1つに記載の方法において、T r E およびH e N B は、鍵を、通信を保護するために、また、相互認証のために使う方法。

【0298】

10

20

30

40

50

106. 実施形態57～105のいずれか1つに記載の方法において、デバイス妥当性確認のためのIKEv2プロトコルは、HeNBへのTrEのバインドに使われる方法。

【0299】

107. 実施形態57～106のいずれか1つに記載の方法において、デバイス完全性は、デバイス完全性の妥当性確認およびデバイス認証のプロシーダを結びつけることによって、デバイスIDにバインドされる方法。

【0300】

108. 実施形態57～107のいずれか1つに記載の方法において、デバイス完全性の妥当性確認およびデバイス認証は、保護されたTrE内部で実施される方法。

【0301】

109. 実施形態57～108のいずれか1つに記載の方法において、TrEは、保護された、信頼できるエンティティである方法。

【0302】

110. 実施形態57～109のいずれか1つに記載の方法において、TrEは、デバイス完全性の妥当性確認およびデバイス認証のプロシーダを実行する方法。

【0303】

111. 実施形態57～110のいずれか1つに記載の方法において、IKEv2プロトコルのセッション、または直後のセッションは、デバイス完全性の妥当性確認およびデバイス認証両方に使われる方法。

【0304】

112. 実施形態57～111のいずれか1つに記載の方法において、デバイス妥当性確認プロシーダを新規メッセージ交換に組み合わせることをさらに含む方法。

【0305】

113. 実施形態57～112のいずれか1つに記載の方法において、新規要求および応答交換は、デバイス認証のために実施される別の同様の交換に先行する方法。

【0306】

114. 実施形態57～113のいずれか1つに記載の方法において、デバイス認証によって使われる要求および応答交換は、デバイス妥当性確認プロシーダに使われる方法。

【0307】

115. 実施形態57～114のいずれか1つに記載の方法において、デバイス完全性の妥当性確認に必要とされる追加データは、選ばれたメッセージフィールドに組み込まれる方法。

【0308】

116. 実施形態57～115のいずれか1つに記載の方法において、デバイス完全性に必要とされるデータは、ローカル自律完全性チェックまたは半自律的妥当性確認の出力結果についての署名されたステートメントを含む方法。

【0309】

117. 実施形態57～116のいずれか1つに記載の方法において、メッセージフィールドは、保護された通知フィールドを含む方法。

【0310】

118. 実施形態57～117のいずれか1つに記載の方法において、デバイス妥当性確認プロシーダを既存のメッセージ交換に組み合わせることをさらに含む方法。

【0311】

119. 実施形態57～118のいずれか1つに記載の方法において、デバイス妥当性確認プロシーダを新規要求および応答交換に組み合わせることをさらに含む方法。

【0312】

120. 上記実施形態のいずれかに記載の方法において、完全性チェックを実施し、完全性チェックで生じた情報を用いて、ネットワーク決定に影響を与えることをさらに含む方法。

10

20

30

40

50

【0313】

121. 上記実施形態のいずれかに記載の方法において、情報要素は、製造元および完全性アルゴリズムを含む方法。

【0314】

122. 上記実施形態のいずれかに記載の方法において、コンポーネント特有の情報要素は、コンポーネント説明、コンポーネント識別（ID）および信頼できる参照値（TRV）を含む方法。

【0315】

123. 上記実施形態のいずれかに記載の方法において、モジュール特有の情報要素は、モジュール説明、モジュール識別（ID）、機能説明、機能ID、コンポーネントID、リリースバージョンおよび重大度を含む方法。

10

【0316】

124. 上記実施形態のいずれかに記載の方法において、重大度は、完全性チェックの失敗の影響を指定する方法。

【0317】

125. 上記実施形態のいずれかに記載の方法において、重大度は、1から4のスケールで分類される方法。

【0318】

126. 上記実施形態のいずれかに記載の方法において、重大度1は、H(e)NB機能性に対する高い影響を表明し、停止動作を保証することができ、フォールバックコードイメージ（FBC）は、指定されたH(e)MSに非常信号を送ることができる方法。

20

【0319】

127. 上記実施形態のいずれかに記載の方法において、重大度2は、制限されたH(e)NB機能性を表明する方法。

【0320】

128. 上記実施形態のいずれかに記載の方法において、3の重大度は、コア機能性に影響を与えなくてよく、モジュール／機能の失敗は、ファームウェアアップデートプロセスで置き換えられ、リブートにより妥当性確認される方法。

【0321】

129. 上記実施形態のいずれかに記載の方法において、4の重大度は、コア機能性に影響を与えなくてよく、失敗したモジュールは、通常ファームウェアアップデートを介して置き換えることができる方法。

30

【0322】

130. 上記実施形態のいずれかに記載の方法において、自律的妥当性確認中、デバイス完全性チェックはローカルに実施される方法。

【0323】

131. 上記実施形態のいずれかに記載の方法において、完全性チェックが失敗するという条件で、非常信号が宅内移動局（H(e)MS）に送られる方法。

【0324】

132. 上記実施形態のいずれかに記載の方法において、半自律的妥当性確認中、完全性チェックに失敗した機能性のリストは、パーソナルビデオエンコーダ（PVE）に報告される方法。

40

【0325】

133. 上記実施形態のいずれかに記載の方法において、完全性チェック中、モジュールは一度だけ調べられる方法。

【0326】

134. 上記実施形態のいずれかに記載の方法において、モジュールは、ただ1つのコンポーネントにおいて現れる方法。

【0327】

135. 上記実施形態のいずれかに記載の方法において、モジュールは、2つの機能の

50

間で共有され得る方法。

【0328】

136. 上記実施形態のいずれかに記載の方法において、各モジュールは、関連付けられた機能性をもち、失敗した機能性のリストは、半自律的妥当性確認（SAV）において導出され、パーソナルビデオエンコーダ（PVE）に送られ得る方法。

【0329】

137. 上記実施形態のいずれかに記載の方法において、機能性識別子（ID）は、モジュールの分類を与える方法。

【0330】

138. 上記実施形態のいずれかに記載の方法において、モジュールは、生成されたイメージに基づいて分類される方法。

10

【0331】

139. 上記実施形態のいずれかに記載の方法において、モジュールのグループは、同じコンポーネント識別子（ID）を含み、まとめて完全性をチェックされる方法。

【0332】

140. 上記実施形態のいずれかに記載の方法において、1つのコンポーネント識別子（ID）をもつモジュールは、異なる機能性識別子（ID）で分類される方法。

【0333】

141. 上記実施形態のいずれかに記載の方法において、モジュール識別子（ID）は、様々なソフトウェアモジュールを追跡するのに使われ、標準化されない方法。

20

【0334】

142. 上記実施形態のいずれかに記載の方法において、モジュールは、機能性および完全性チェック単位に基づいて分類される方法。

【0335】

143. 上記実施形態のいずれかに記載の方法において、同じコンポーネント識別子（ID）をもつ全モジュールは、1つの信頼できる参照値をもち、信頼できる参照値が失敗するという条件で、失敗したコンポーネントの全モジュールは、失敗した機能性のリストを判定するのに使われ、宅内移動局（H(e)MS）またはパーソナルビデオエンコーダ（PVE）に伝達される方法。

【0336】

144. 上記実施形態のいずれかに記載の方法において、機能性のリストは、コンポーネントに関連付けられる方法。

30

【0337】

145. 上記実施形態のいずれかに記載の方法において、コンポーネントは、ロードされる順序で編成される方法。

【0338】

146. 上記実施形態のいずれかに記載の方法において、完全性チェックは、イメージオブジェクトファイルの一部に対して実施され、イメージオブジェクトファイルが完全性チェックを通らないという条件で、失敗したセグメント名が抽出される方法。

【0339】

147. 上記実施形態のいずれかに記載の方法において、CPE（顧客構内設備）は、信頼できる参照をH(e)NBにダウンロードするのに使われ、信頼できる参照は、ネットワークオペレータの署名鍵によってデジタル署名される方法。

40

【0340】

148. 上記実施形態のいずれかに記載の方法において、信頼できる参照値を含む署名されたパケットを受信すると、H(e)NBは、署名を復号し、受信された信頼できる参照値の真正性および完全性を検証する方法。

【0341】

149. 上記実施形態のいずれかに記載の方法において、信頼できる参照値は、デジタル署名される前に、機密性のために暗号化される方法。

50

【0342】

150. 上記実施形態のいずれかに記載の方法において、信頼できる参照値は、ソフトウェアモジュールバイナリイメージの一部に付加される方法。

【0343】

151. 上記実施形態のいずれかに記載の方法において、H(e)NBおよび宅内移動局H(e)MSは、SSL/TLS（セキュアソケットレイヤ/トランスポートレイヤセキュリティ）をサポートし、証明書ベースの認証を使う方法。

【0344】

152. 上記実施形態のいずれかに記載の方法において、TR069ベースのアーキテクチャは、証明書ベースの認証をサポートする方法。

10

【0345】

153. 上記実施形態のいずれかに記載の方法において、H(e)NBは、Management Server. URLパラメータ中のデフォルトの宅内移動局H(e)MS URL（ユニフォームリソースロケータ）で構成される方法。

【0346】

154. 上記実施形態のいずれかに記載の方法において、H(e)NBは、LAN（ローカルエリアネットワーク）側Management Server. URL構成をサポートする方法。

【0347】

155. 上記実施形態のいずれかに記載の方法において、セキュリティゲートウェイ（SeGW）URL（ユニフォームリソースロケータ）はパラメータである方法。

20

【0348】

156. 上記実施形態のいずれかに記載の方法において、自律的妥当性確認中に、デジタル署名またはメッセージは私有鍵を使って署名される方法。

【0349】

157. 上記実施形態のいずれかに記載の方法において、自律的妥当性確認中に、情報はネットワークエンティティに送られない方法。

【0350】

158. 上記実施形態のいずれかに記載の方法において、最低要件は、信頼できる参照完全性メトリックまたは信頼できる参照値の生成に使われるアルゴリズム向けに標準化される方法。

30

【0351】

159. 上記実施形態のいずれかに記載の方法において、信頼できる参照値は、信頼できるサードパーティによって生成され、デジタル署名される方法。

【0352】

160. 上記実施形態のいずれかに記載の方法において、ローカル完全性データ初期化が実施される方法。

【0353】

161. 上記実施形態のいずれかに記載の方法において、構成データの初期プロビジョニングが実施される方法。

40

【0354】

162. 上記実施形態のいずれかに記載の方法において、参照完全性メトリックは、信頼できる参照値になる方法。

【0355】

163. 上記実施形態のいずれかに記載の方法において、デバイス構成データシートは、デバイスの安全なメモリ内部で維持され、認可された当事者によってアクセスされる方法。

【0356】

164. 上記実施形態のいずれかに記載の方法において、デバイス構成データは、H(e)NBによって暗号化され復号される方法。

50

【0357】

165. 上記実施形態のいずれかに記載の方法において、安全なブートプロセス中、生成されたダイジェストは、デバイス構成データシート中で指定された値と比較される方法。

【0358】

166. 上記実施形態のいずれかに記載の方法において、デバイス構成データシートが失効するという条件で、H(e)NBがファームウェアアップデートプロセスを開始して、修復サーバからデータをプルする方法。

【0359】

167. 上記実施形態のいずれかに記載の方法において、宅内移動局(H(e)MS)は、RPC(リモートプロシージャコール)を開始し、Management Server URLをアップデートする方法。

10

【0360】

168. 上記実施形態のいずれかに記載の方法において、ファイルを転送するために、FTPS(ファイル転送プロトコルセキュア)が実装される方法。

【0361】

169. 上記実施形態のいずれかに記載の方法において、デバイス完全性チェックは、自律的妥当性確認において失敗し、ローカル非常フラグが設定され、フォールバックコード(FBC)がデバイスに格納される方法。

【0362】

170. 上記実施形態のいずれかに記載の方法において、非常信号は、デバイス完全性チェック失敗の詳細を含む方法。

20

【0363】

171. 上記実施形態のいずれかに記載の方法において、FTP(ファイル転送プロトコル)サーバは、宅内移動局(H(e)MS)とマージされる方法。

【0364】

172. 上記実施形態のいずれかに記載の方法において、半自律的妥当性確認(SAV)中、H(e)NBは、安全でないリンクを介して、安全なゲートウェイ(SeGW)と対話する方法。

【0365】

173. 上記実施形態のいずれかに記載の方法において、安全なゲートウェイ(SeGW)は、認証されたH(e)NBのみがネットワークにアクセスすることを許可する方法。

30

【0366】

上記実施形態のいずれかに記載の方法において、宅内移動局(H(e)MS)は、H(e)NB管理サーバとして作用し、修復のサポートを提供する方法。

【0367】

174. 上記実施形態のいずれかに記載の方法において、SAVにおいて、H(e)NBは、予め指定されたコンポーネントの完全性の検査を実施する方法。

【0368】

175. 上記実施形態のいずれかに記載の方法において、SAVにおいて、コンポーネントの認証は、完全性アルゴリズムからのダイジェスト出力を、デバイス構成シート中の指定された値と比較することによってローカルに実施される方法。

40

【0369】

176. 上記実施形態のいずれかに記載の方法において、H(e)NBのトランスポート要素(TrE)は、予め定義されたコンポーネントの完全性の検査を実施する方法。

【0370】

177. 上記実施形態のいずれかに記載の方法において、H(e)NBは、証明書交換による安全なゲートウェイ(SeGW)で、IKE(インターネット鍵交換)セキュリティアソシエーションを確立する方法。

50

【0371】

178. 上記実施形態のいずれかに記載の方法において、コンポーネントのローカル完全性の妥当性確認の後、コンポーネントがデバイスによってロードされ実行される方法。

【0372】

179. 上記実施形態のいずれかに記載の方法において、インターネット鍵交換（IKE）要素が送られて、暗号アルゴリズム用のセキュリティパラメータ索引を含むセキュリティアソシエーションを確立する方法。

【0373】

180. 上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（SeGW）は、IKE（インターネット鍵交換）に対する応答を送る方法。

10

【0374】

181. 上記実施形態のいずれかに記載の方法において、H（e）NBは、証明書を、相互認証のためのIKE__AUTH__REQに入れて送る方法。

【0375】

182. 上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（SeGW）は、H（e）NBの認証資格を評価し、機能性識別子のリストを抽出する方法。

【0376】

183. 上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（SeGW）は、認証妥当性確認が成功した場合はH（e）NBに指示を送る方法。

【0377】

184. 上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（SeGW）は、認証妥当性確認が失敗した場合はH（e）NBに指示を送る方法。

20

【0378】

185. 上記実施形態のいずれかに記載の方法において、SeGWは、失敗した機能性のリストをパーソナルビデオエンコーダ（PVE）に送る方法。

【0379】

186. 上記実施形態のいずれかに記載の方法において、PVEは、デバイスの検疫、完全アクセスの提供、部分アクセスの提供または修復のための宅内移動局（H（e）MS）介入の要求を含むアクションを判定する方法。

【0380】

187. 上記実施形態のいずれかに記載の方法において、PVEは、決定をSeGWに通知する方法。

30

【0381】

188. 上記実施形態のいずれかに記載の方法において、パーソナルビデオエンコーダ（PVE）は、修復をスタートするための通知および失敗したモジュールのリストを宅内移動局（H（e）MS）に送る方法。

【0382】

189. 上記実施形態のいずれかに記載の方法において、パーソナルビデオエンコーダ（PVE）は、修復に関する通知をH（e）NBに送る方法。

【0383】

190. 上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（SeGW）は、デバイス完全性評価の結果をH（e）NBに示す方法。

40

【0384】

191. 上記実施形態のいずれかに記載の方法において、トランスポート要素（TrE）は、完全性検証を外部エンティティに委任する方法。

【0385】

192. 上記実施形態のいずれかに記載の方法において、H（e）NBは、NTP（ネットワークタイムプロトコル）を使って時間を同期させるローカルタイムサーバを含む方法。

【0386】

50

193. 上記実施形態のいずれかに記載の方法において、S A Vにおける認証証明書およびローカル妥当性確認の結果は、I K E __ A U T H __ R E Qメッセージに入れて送られる方法。

【0387】

194. 上記実施形態のいずれかに記載の方法において、安全なゲートウェイ (S e G W) は、失敗したモジュールの一覧を、リストをパーソナルビデオエンコーダ (P V E) に渡す前にフィルタリングする方法。

【0388】

195. 上記実施形態のいずれかに記載の方法において、H (e) N Bは、安全なゲートウェイを経由して、またはインターネットを介して接続することによって、宅内移動局 (H (e) M S) と対話して、修復をサポートする方法。

10

【0389】

196. 上記実施形態のいずれかに記載の方法において、宅内移動局 (H (e) M S) は、R P C (リモートプロシージャコール) を呼び出して、H (e) N Bが失敗した機能性のリストおよびエラーコードのリストをアップロードすることを示す方法。

【0390】

197. 上記実施形態のいずれかに記載の方法において、宅内移動局 (H (e) M S) は、失敗した機能性のリストのアップロードを準備するよう、F i l e S e v e r に対して指示する方法。

【0391】

20

198. 上記実施形態のいずれかに記載の方法において、H (e) N Bは、失敗した機能性のリストを含むファイルをアップロードするためのプロシージャを呼び出す方法。

【0392】

199. 上記実施形態のいずれかに記載の方法において、F i l e S e v e r は、アップロードされたファイルの評価の後、宅内移動局 (H (e) M S) にD o w n l o a d __ P a c k a g e __ R e a d yメッセージを送る方法。

【0393】

200. 上記実施形態のいずれかに記載の方法において、宅内移動局 (H (e) M S) は、R P C (リモートプロシージャコール) を呼び出し、デバイス構成シートのU R L (ユニフォームリソースロケータ) を与える方法。

30

【0394】

201. 上記実施形態のいずれかに記載の方法において、H (e) N Bは、F T P (ファイル転送プロトコル) ファイルサーバに接続し、ファームウェアイメージおよびデバイス構成シートをダウンロードする方法。

【0395】

202. 上記実施形態のいずれかに記載の方法において、宅内移動局 (H (e) M S) は、成功したダウンロード応答を受信すると、リブートプロシージャを呼び出す方法。

【0396】

203. 上記実施形態のいずれかに記載の方法において、H (e) N Bは、成功したダウンロード応答を受信すると、ローカル非常フラグをリセットする方法。

40

【0397】

204. 上記実施形態のいずれかに記載の方法において、宅内移動局 (H (e) M S) は、デバイスのブートが成功したことを示すメッセージを安全なゲートウェイ (S e G W) から受信する方法。

【0398】

205. 上記実施形態のいずれかに記載の方法において、安全なブートプロセス中に完全性チェックがロードされ実行され、認証の実施が成功するという条件で、H (e) N Bがセキュリティゲートウェイと通信する方法。

【0399】

206. 上記実施形態のいずれかに記載の方法において、ローカル完全性チェックの結

50

果を伝送することをさらに含む方法。

【0400】

207. 上記実施形態のいずれかに記載の方法において、ローカル完全性チェックの結果をパーソナルビデオエンコーダ(PVE)にフォワードすることをさらに含む方法。

【0401】

208. 上記実施形態のいずれかに記載の方法において、H(e)NBは、失敗した機能性のリストおよび製造元固有エラーコードのリストを、IKEv2 NOTI F Yメッセージに入れてSeGWに送る方法。

【0402】

209. 上記実施形態のいずれかに記載の方法において、SeGWは、失敗した機能性のリストをパーソナルビデオエンコーダ(PVE)にフォワードする方法。

10

【0403】

210. 上記実施形態のいずれかに記載の方法において、PVEは、SeGWアクション、H(e)NBアクションを決定し、アクションのリストをSeGWにフォワードする方法。

【0404】

適切なプロセッサは、例として、汎用プロセッサ、特殊目的プロセッサ、従来のプロセッサ、DSP(デジタル信号プロセッサ)、複数のマイクロプロセッサ、DSPコアと関連した1つもしくは複数のマイクロプロセッサ、コントローラ、マイクロコントローラ、ASIC(特定用途向け集積回路)、ASSP(特定用途向け標準製品)、FPGA(フィールドプログラム可能ゲートアレイ)回路、他の任意のタイプのIC(集積回路)、および/または状態マシンを含む。

20

【0405】

ソフトウェアと関連したプロセッサは、WTRU(ワイヤレス送受信ユニット)、UE(ユーザ機器)、端末、基地局、MME(移動管理エンティティ)もしくはEPC(進化型パケットコア)、または任意のホストコンピュータ内で使用するための無線周波数トランシーバを実装するのに使うことができる。WTRUは、SDR(ソフトウェア無線)を含むハードウェアおよび/またはソフトウェア中に実装されるモジュール、並びにカメラ、ビデオカメラモジュール、テレビ電話、スピーカフォン、振動デバイス、スピーカ、マイクロホン、テレビトランシーバ、ハンズフリーヘッドセット、キーボード、ブルートゥース(登録商標)モジュール、FM(周波数変調)無線ユニット、NFC(近距離無線通信)モジュール、LCD(液晶ディスプレイ)表示ユニット、OLED(有機発光ダイオード)表示ユニット、デジタルミュージックプレーヤ、メディアプレーヤ、ビデオゲームプレーヤモジュール、インターネットブラウザ、および/または任意のWLAN(ワイヤレスローカルエリアネットワーク)もしくはUWB(超広帯域)モジュールなど、他のコンポーネントとともに使うことができる。

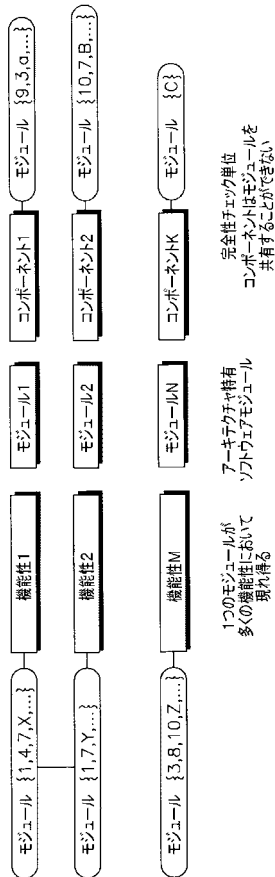
30

【0406】

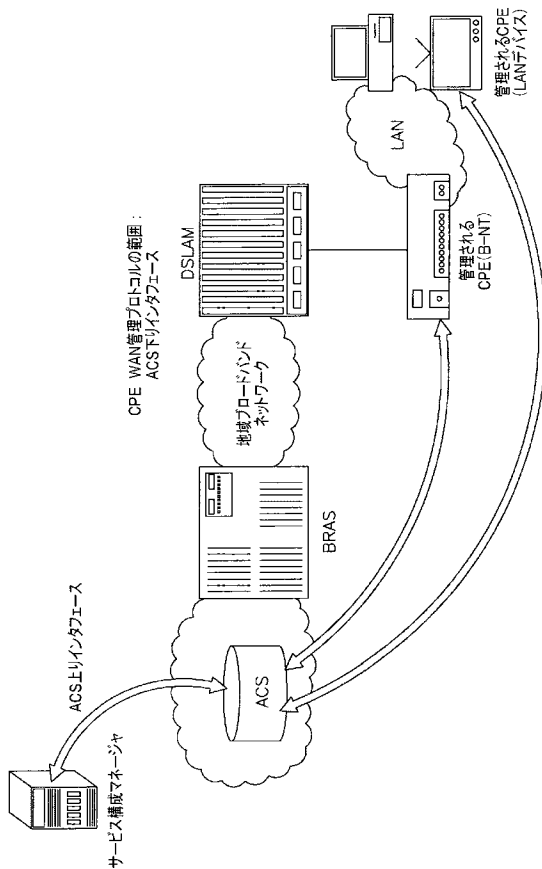
特徴および要素を、具体的に組み合わせて上で記載したが、各特徴または要素は、他の特徴および要素なしで個別に、または他の特徴および要素ありでもなしでも、様々な組み合わせで用いることができる。本明細書に挙げた方法またはフローチャートは、汎用コンピュータまたはプロセッサによる実行用のコンピュータ可読記憶媒体に組み込まれる、コンピュータプログラム、ソフトウェア、またはファームウェア中に実装することができる。コンピュータ可読記憶媒体の例は、ROM(読出し専用メモリ)、RAM(ランダムアクセスメモリ)、レジスタ、キャッシュメモリ、半導体メモリ素子、内部ハードディスクおよび取外し可能ディスクなどの磁気メディア、光磁気メディア、並びにCD-ROMディスク、およびDVD(デジタル多用途ディスク)などの光メディアを含む。

40

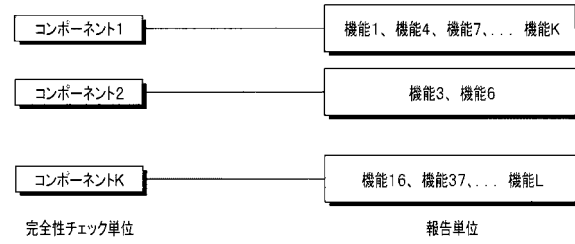
【図 1】



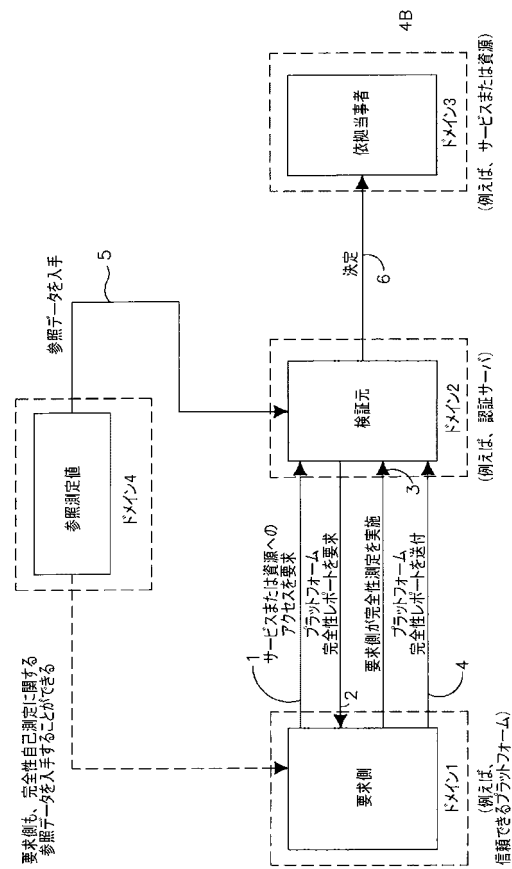
【図 3】



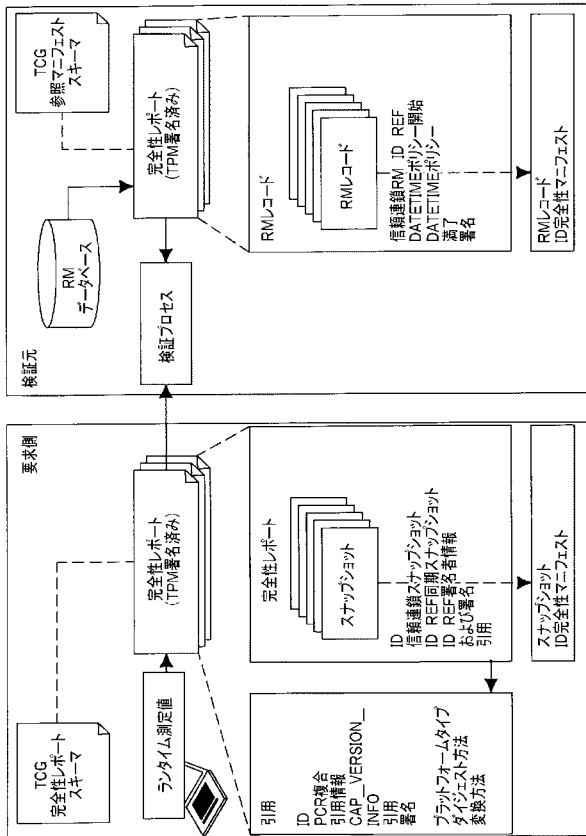
【図 2】



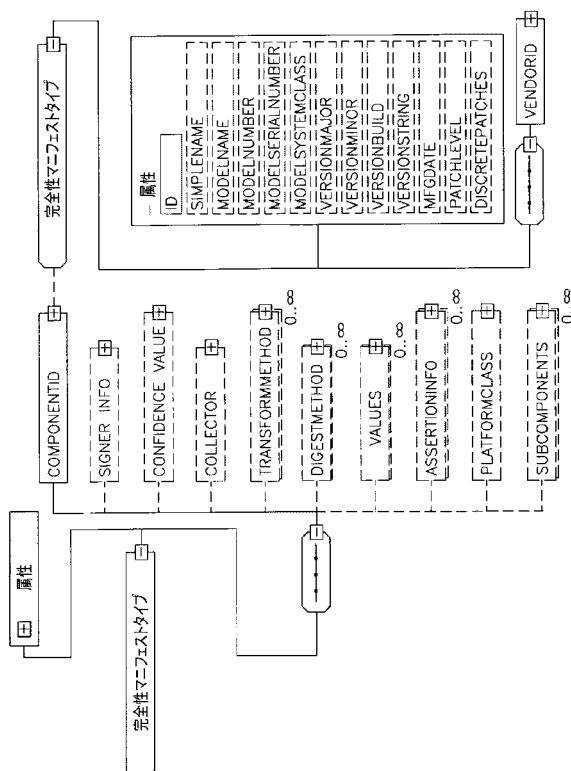
【図 4】



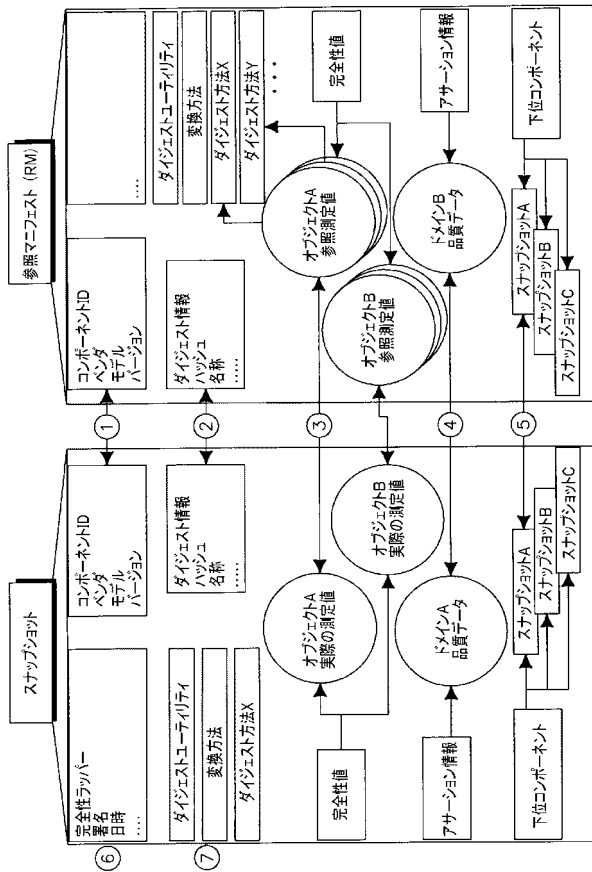
【 図 5 】



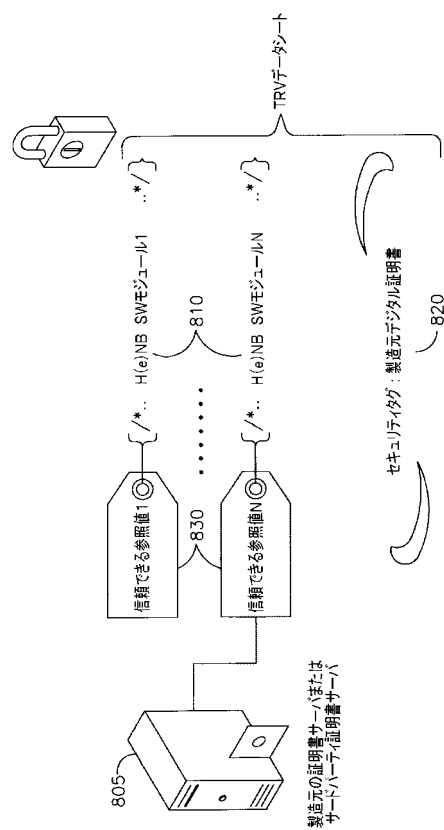
【 図 7 】



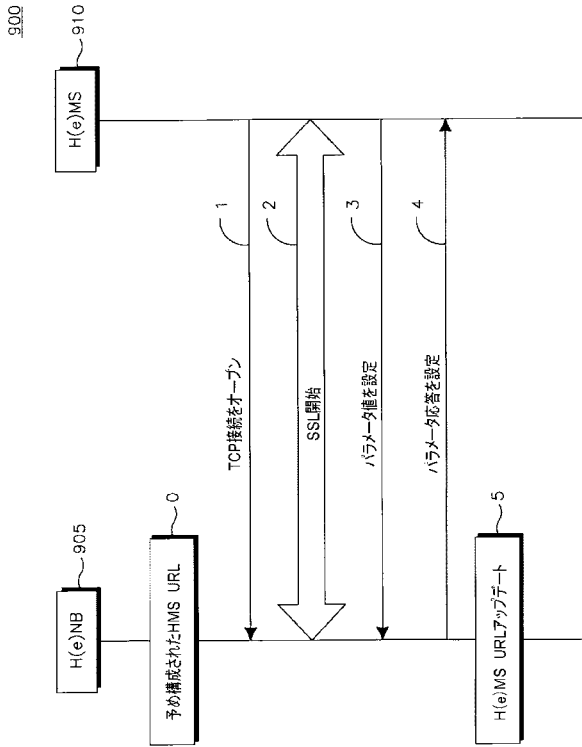
【図 6】



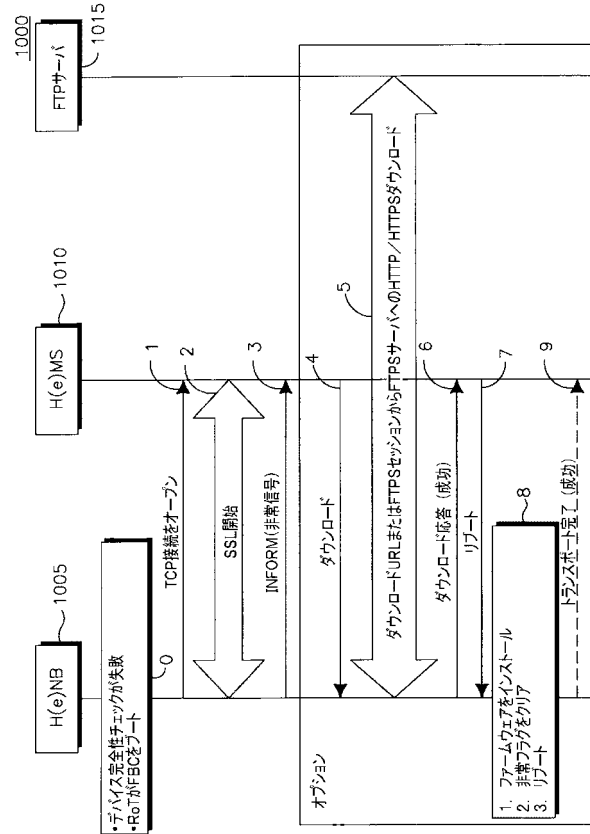
【图 8】



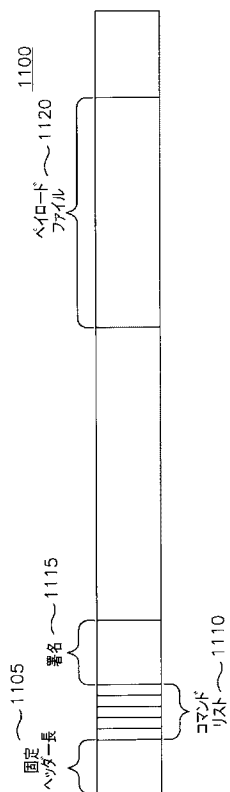
【図 9】



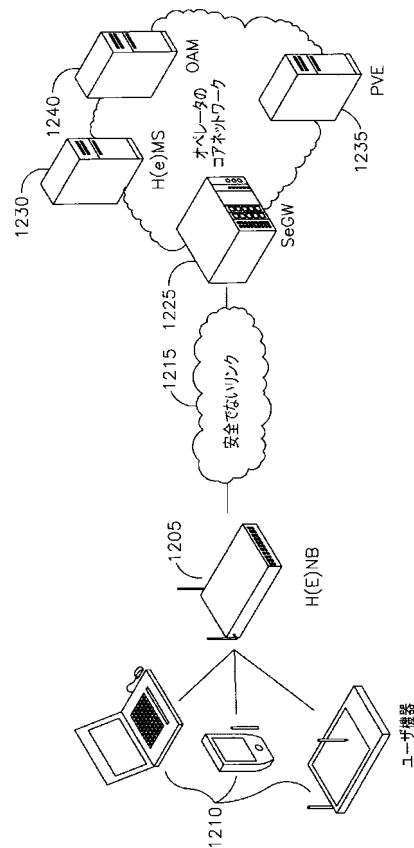
【図 10】



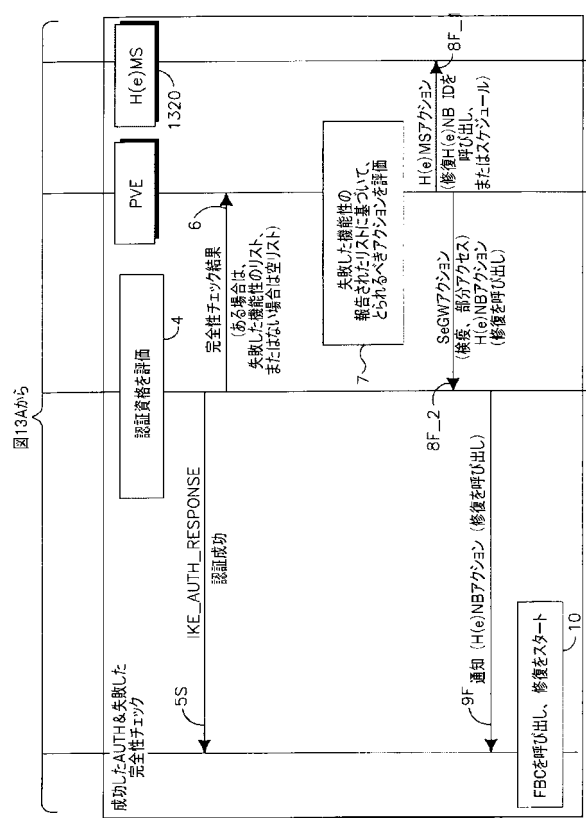
【図 11】



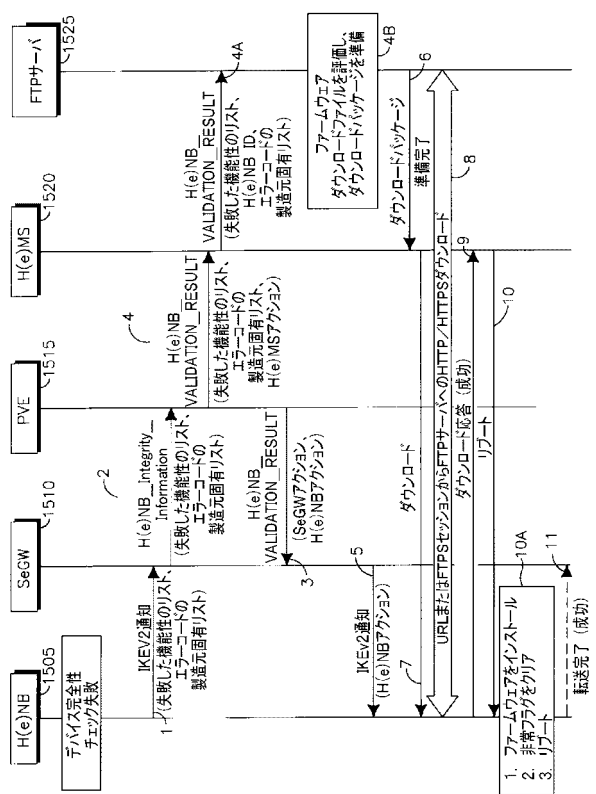
【図 12】



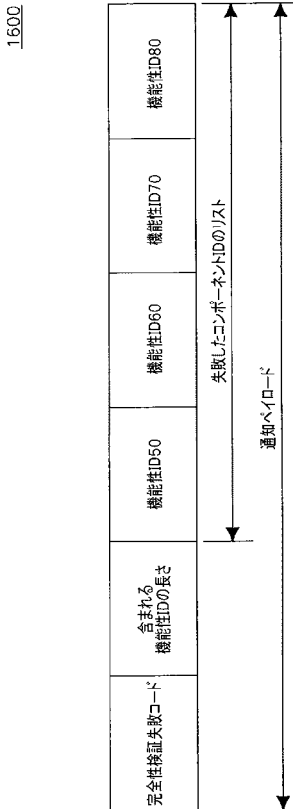
【图 1 3 B】



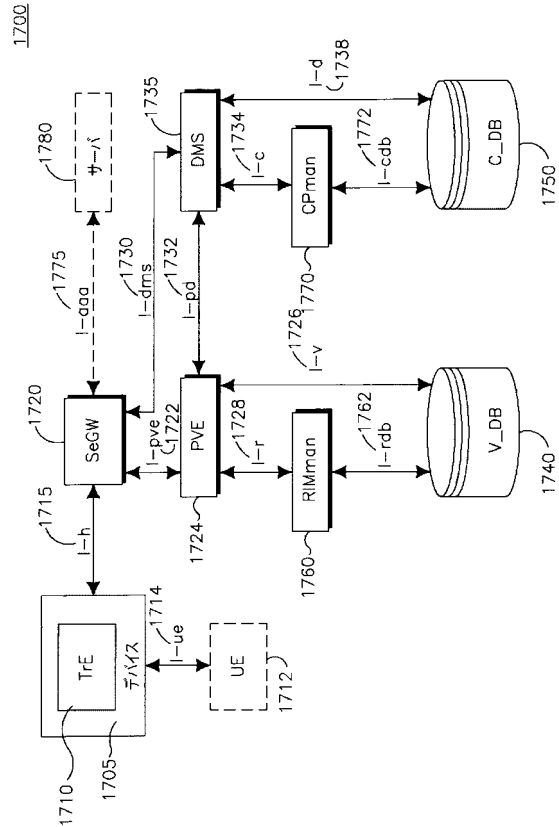
【 図 1 5 】



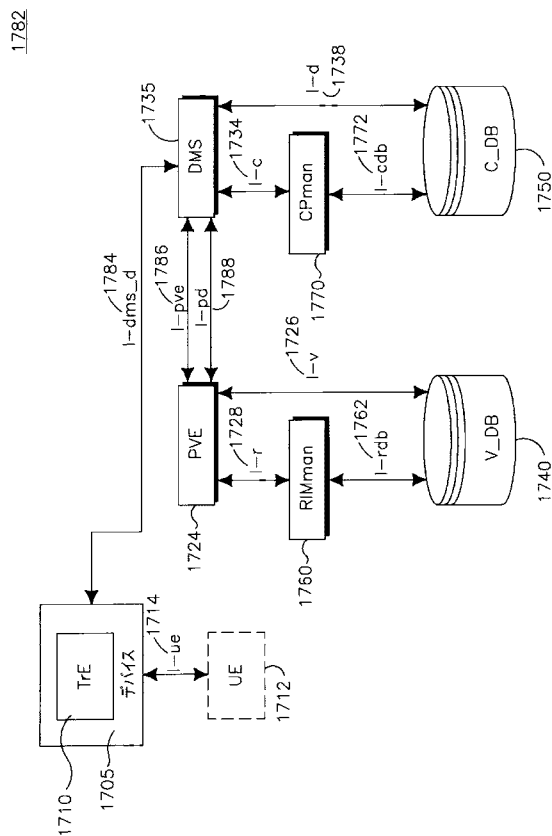
【図 16】



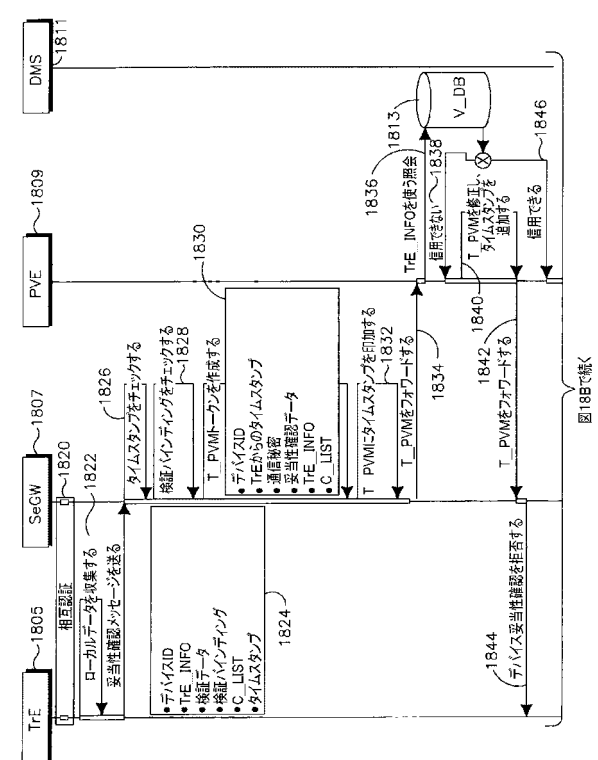
【図 17 A】



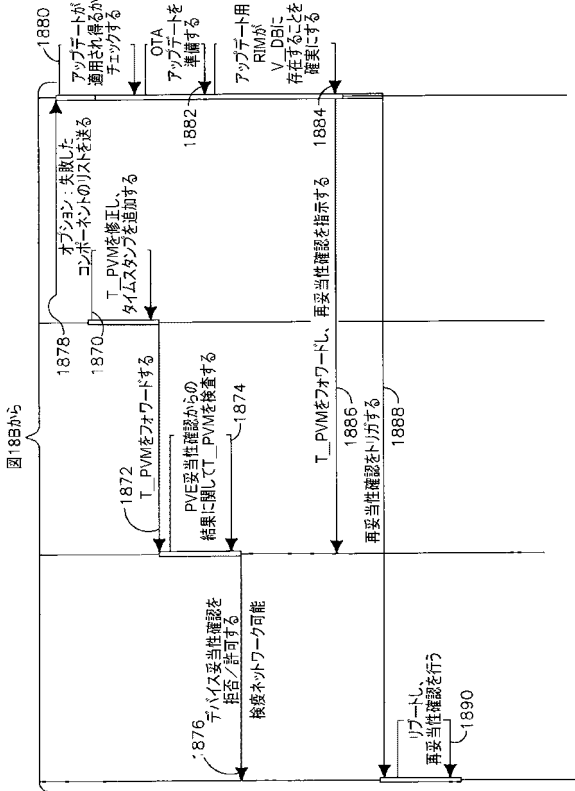
【図 17 B】



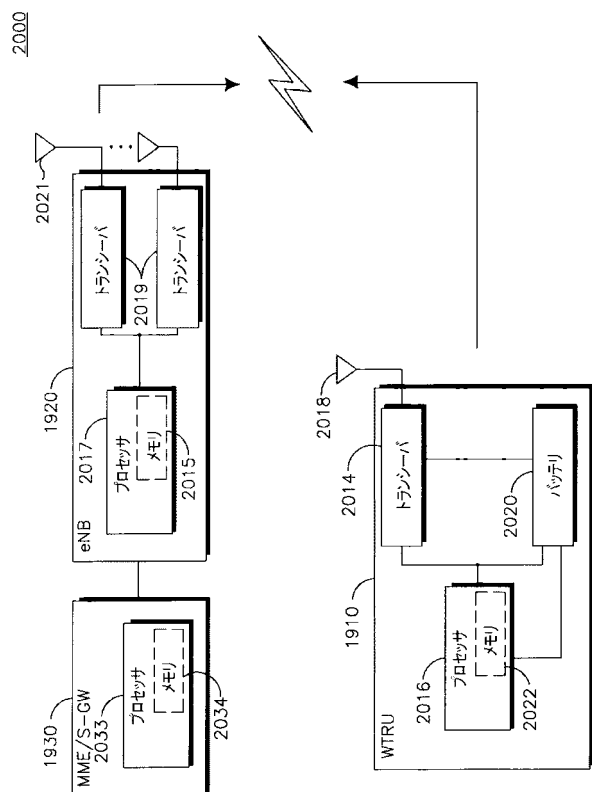
【図 18 A】



【図 18 C】



【图 20】



フロントページの続き

(51)Int.Cl.	F I	テーマコード (参考)
G 0 6 F 21/64 (2013.01)	G 0 6 F 21/50	
	G 0 6 F 21/64	

(31)優先権主張番号 61/239,698

(32)優先日 平成21年9月3日(2009.9.3)

(33)優先権主張国 米国(US)

(72)発明者 インヒョク チャ

アメリカ合衆国 19067 ペンシルベニア州 ヤードリー サウスリッジ サークル 510

(72)発明者 アンドレアス ユー. シュミット

ドイツ 65929 フランクフルト アム マイン トイトーネン 37

(72)発明者 アンドレアス レイチェル

ドイツ 60488 フランクフルト アム マイン ガイスフェルトストラッセ 2

(72)発明者 ヨゲンドラ シー. シャー

アメリカ合衆国 19341 ペンシルベニア州 エクストン リージェンシー コート 10

(72)発明者 ドロレス エフ. ハウリー

アメリカ合衆国 19087 ペンシルベニア州 ウェイン ウォーレス ドライブ 680

(72)発明者 デービッド ジー. グレイナー

アメリカ合衆国 11040 ニューヨーク州 ニュー ハイド パーク ヨークシャー ロード
57

(72)発明者 ローレンス エル. ケース

アメリカ合衆国 19468 ペンシルベニア州 ロイヤーズフォード モーガン ドライブ 3
07

(72)発明者 マイケル ブイ. マイヤーステイン

イギリス アイピー5 3ティーユー イプスウィッチ マートルシャム ヒース メイフィール
ズ 27

(72)発明者 ルイス ジェイ. グッチョーネ

アメリカ合衆国 10709 ニューヨーク州 イースト チェスター リンカーン プレイス
211

Fターム(参考) 5J104 AA08 LA02 LA03 LA06 NA02 NA37 PA02

5K067 AA30 EE10 HH22 HH23