GCOT Open RANに関する認証原則【仮訳】

1. はじめに

1.1. 背景

移動通信による無線アクセス網(Radio Access Network: RAN)は非常に複雑な機能である。RANには、顧客の要求を満たし、ネットワークが高い「アップタイム（連続稼働時間)」を維持するための、非常に高いパフォーマンス要件が存在する。また、RANは、ユーザーの位置や移動中か否かに関係なく、シームレスに操作できることへの要求に基づき、広い地理的範囲をカバーすることが多々ある。この結果、歴史的に、サプライヤーが RAN に関してシングルベンダーのソリューションを提供することにつながると同時に、産業の集中が生じた。

Open RAN（Open Radio Access Network）は、こうした状況への代替案を提供する、電気通信業界における進展の代表的なものである。これは、SDN（Software-Defined Networking）やNFV（Network Functions Virtualization）等の技術とともに、2010 年代初頭に登場した、ハードウェアとソフトウェアの分離を目指す技術である。5G 標準規格に係る最初のフェーズである 3GPP の「Release15」は、柔軟性とモジュール性を強調した、5G通信網における基本枠組みを確立することによって、Open RAN に大きな影響を与えた。「Release15」では、CU（Centralized Unit)、DU（Distributed Unit)、RU（Radio Unit）等の、Open RANにおける主要な機能とインターフェースの考え方が導入され、RANの分散を可能とした。さらに、O-RAN ALLIANCE は、DU と RU の間にフロントホールインターフェースを定義することで、この柔軟性をさらに拡大し、事業者が複数のベンダーのソリューションを統合できるようにした。O-RAN ALLIANCEは、これに加え、RIC（RAN インテリジェントコントローラー）を非リアルタイムとリアルタイムに規格化した。これにより、3GPP で定義されたものを超えた、追加の性能や機能を必要とする、特定のユースケースに合わせて、RANをカスタマイズ可能となった。

3GPPとO-RAN ALLIANCEによる協力の結果、モバイル事業者は現在、RANの設計、ベンダーの選択、無線機能のカスタマイズについて、複数の選択肢を持っている。この新たに得られた柔軟性は、マルチベンダーによるソリューションを統合する際の複雑さや潜在的な相互運用性の問題をもたらす。

1.2. Open RANにおける認証の必要性

商用展開に向けて、Open RANソリューションは、相互運用可能で、高い適合性とパフォーマンスを持ち、安全である必要がある。一方で、RAN の複雑さを考慮すると、Open RANソリューションがこれらの基準を確実に満たすことは困難なことでもある。移動体通信事業者（Mobile Network Operators：MNO）には、統合された各Open RANソリューションを個別にテストするためのリソースが不足している可能性がある。また、Open RANのサプライヤーは、特にサプライヤーが実証コストを負担することが期待される場合等においては、すべての潜在

的な顧客に対し、相互運用性、適合性、パフォーマンス、及びセキュリティを個別に実証することができない可能性がある。

従って、Open RAN 市場において、顧客が適合性、相互運用性、パフォーマンスに十分に優れた製品を入手できるという信頼性を与えるためには、認証制度が必要となることは明らかである。これは、農業、製造業、鉱業等の特定の業界が Open RAN ネットワークを導入し、従来の MNO とは異なる運用をサポートすることが想定される、新興のプライベートワイヤレス市場にとって特に重要となる。一方で、認証はこれらの課題のいくつかに対処するのに役立つものの、これ単独では Open RAN 展開の複雑さとリソースの要求のすべてを解決することはできない。Open RAN エコシステムは、これまでに確立されたあらゆる認証プログラムにから、今後も革新と反復による改善を続ける必要がある。

既存の認証プログラム、例えば、TIP (Telecom Infra Project) と O-RAN ALLIANCE によって開発されているもの等は、これらの課題に対処するための重要な第一歩を踏み出すものである。本書で概説される原則は、こうした制度の有効性を、今後最大化するための枠組みを提供するために、既存の試験及び認証業務を基礎としたい。

1.3. 目的

本文書は、GCOT を代表して、Open RAN エコシステムのステークホルダーが、Open RAN 機器のための強固で包括的な認証プログラムを開発するための、自発的な枠組みを提示することを目的としている。これは、この目的を達成するために必要なステップに関するアイディアを提供し、それに向けて次のステップを実現する方法について、産業界との議論を容易にするためのものである。ただし、本文書は、Open RAN 認証プログラムそのものではなく、認証プログラムをどのように構築するかに関する完全な手順のリストでもない。

1.4. 対象

本文書の対象は、Open RAN エコシステムのステークホルダー(MNO、Open RAN ハードウェア及びソフトウェアのサプライヤー、インフラ提供者、システムインテグレーター、Open RAN 認証プログラムの開発・運用に関与する可能性のあるその他の組織)である。

2. 認証のガバナンスとインテグリティ

2.1. 役割と責任

すべてのステークホルダーの役割と責任を明確に定義することは、Open RAN の採用を促進するための重要な要素である。

- *MNO* は、認証を受けた Open RAN ソリューションを、個別のネットワーク要件及びパフォーマンス目標に合わせ選択する。可能な場合には、製品開発と有用なパフォーマンステストを可能にするために、これらの要件を公開する。

- *ハードウェア/ソフトウェア製造者*は、確立された認証基準に準拠した Open RAN 準拠機器を革新・開発する。彼らは、これらが理論上だけでなく、実際に相互運用可能であることを明らかにする必要がある。
- *パッシブインフラ提供者*は、試験で使用される、典型的な Open RAN ネットワークの運用・保守に必要な物理リソース及び仮想リソースを提供できる。これには、ファイバー、通信塔、データセンター、クラウドサービス等が含まれる。
- *システムインテグレーター*は、ネットワークアーキテクチャ内で、異なるベンダーの認証取得済み Open RAN 構成機器を、シームレスに統合できる。システムインテグレーターは、特定のベンダーのみがシステム内で使用できる、いわゆる「相互運用性の孤島（islands of interoperability)」ではなく、中立的な実装が可能な、オープンなシステムを作るべきである。
- *認証機関*は、Open RAN 認証のプロセス全体を確立し、管理する。これには、認証要件の定義、試験結果の確認、及び認証の付与が含まれる。
- *テストラボ*は、確立された標準、主要業績評価指標(KPI)、及びセキュリティレベルに照らし、Open RAN 機器の厳格なテストを実施する。
- *政府*は、認証制度の開発や運営、あるいは試験を主導すべきではなく、これは産業界主導のプロセスであるべきである。一方で、場合によっては、政府その他の公的機関が、ロバスト性を確保し、公益の代表性、そして制度の利用が最大化されることを保証するために、(サイバーセキュリティ組織等を通じた)開発プロセスや、(公的に資金提供された研究所等)認証を発行する基金組織への参加をすることも考えられる。また、公共部門及び軍での Open RAN 採用のために、認証された製品を要件とすることも考えられるが、政府による取組については、各政府が個別に決定するものとする。

2.2. 認証のソース

認証制度は、必要な認証試験を開発するために、3GPP や O-RAN ALLIANCE 等の既存の標準及び仕様組織と連携する必要がある。これらは、試験施設全体で標準的なものであり、また、可能であれば、固有の、特異な、あるいは自己開発の試験を、(例えば、特定の地域等において)追加する必要がないように開発されるべきである。3GPP と O-RAN ALLIANCE の両方で、分散型 RAN のテスト仕様が作成されている。例えば、3GPP の TS38.141 は、NR 基地局のための適合性試験を定義する。また、O-RAN ALLIANCE の WG4、WG5 及び WG6 仕様は、Open RAN コンポーネントの適合性、統合、及びセキュリティの試験に焦点を当てている。こうした製品は、Open RAN 認証プログラムの構築に活用できる。

2.3. 試験の種類

認証試験は、適合性、相互運用性、及びパフォーマンスの主要な領域に焦点を当てる必要がある。これらはそれぞれ、Open RAN ソリューションの導入可能性を確保するうえで、重要な役割を果たす。

- **適合性**試験は、インターフェース、サブシステム、及びエンドツーエンドシステムが、適切な規格及び仕様に関する団体によって作成された仕様に準拠しているかを確認する。これには、RU、DU、及び CU の適合性テストが含まれ、RF 処理、ベースバンド処理、及び制御/ユーザープレーン機能の、標準への準拠性を確認する。また、フロントホール(下位レイヤスプリット、上位レイヤスプリット等)、ミッドホール(F1 等)、バックホール(E1 等)、及びその他の管理プレーン(O1 等)やサービス管理インターフェース(A1、E2 等)等のインターフェースの検証も行う。

- **相互運用性**試験では、異なるベンダーのコンポーネントが Open RAN エコシステム内でシームレスに連動できることを検証する。この試験では、RU、DU、CU、及びその他のネットワーク要素が、定義された標準及びプロトコルに準拠していることを確認する。これにより、互換性の問題が発生することなく、各ネットワーク要素が効果的に通信し、運用されることを可能にする。また、フロントホール、ミッドホール、バックホール等のインターフェースの検証も行い、さまざまな設定・実装に渡り相互運用性をサポートする。

- **パフォーマンス**試験では、顧客(MNO 等)が定義した要件、KPI、及び機能に焦点を当てる必要がある。これらは、意味のあるものとなるために、特定のユースケース、構成、及び導入環境に対して、十分に調整される必要がある一方で、過度に特有なものとなることを避ける必要がある。

- **セキュリティ**試験は、各地域の法的及び規制上のセキュリティ要件を遵守し、適合性テストのさまざまな側面を網羅する必要がある。特定のユースケースに合わせて、追加のセキュリティテストを調整することも可能である。この試験では、O-RAN ALLIANCE の WG11 セキュリティワーキンググループや 3GPP の SCAS (Security Assurance Specification) 試験で概説されているベストプラクティスや、NIST、IEC、ETSI 等の組織のセキュリティ枠組みを取りこむ。一般に、合格/不合格形式の認証ではなく、情報に基づいた評価アプローチによって、セキュリティ対策の包括的な評価が保証される。一方で、全体的な評価の一部として合格するために最低限の基準を必要とする場合もありうる。

2.4. 監視

Open RAN 認証制度の開発、ガバナンス、及び監視は、この制度が支える多様な市場を反映したものであるべきであり、特定の市場または地域に偏ったものであってはならない。認証制度に関与している既存の業界団体は、必要なレベルの監視を行うための十分な設備を備えているが、特定の地域あるいは業界等、所与のステークホルダーの意見を過剰または過少に反映することによって、活動にバイアスが生じる可能性に注意を払うべきである。

2.5. 透明性

認証制度を開発する業界団体は、オープンで厳格なアプローチを採用すべきである。これにより、新たな参加者が公正に参入できるようになるとともに、公的機関によるものも含め、外部からの精査が可能になる。公的機関による認証プロセスへのアクセスは、2021 年の「電気通信サプライヤーの多様性に関するプラハ提案」[1]に沿って、認証制度がサイバーセキュリティのベストプラクティスを組み込むことを確実にするために、また、追加的なインターフェースの開放がある場合にも、オープンな取組によって全体的なセキュリティが強化されることを確実にするために必要である。認証を主導する責任及び義務は業界にあるが、外部からの精査により、好ましい成果を支持し保証することができる。

2.6. 適合性評価機関の認証

適合性評価機関(CAB)は、製品、サービスまたはシステムが特定の基準及び規制に適合しているかどうかを評価・認証する、試験所、認証機関等の組織である。発行される認証書は、他の認可された試験所によって、独立に検証可能かつ再現可能である必要がある。これにより、一貫性が保証され、特定のテスト環境に固有のエラーのリスクが最小限に抑えられる。これは、本文書 2.2 に従い、地理的条件に関係なく、一貫性のある標準的なテストプロトコルを使用して保証される必要がある。さらに、試験所は、ISO/IEC17025 及び認証機関に関して ISO/IEC17065 等、業界のベストプラクティス及び標準に従って認可される必要がある。このアプローチでは、取組の重複も避ける必要がある（例えば、米国の CAB によって発行された証明書は、欧州市場において、現地で発行された証明書と同等の信頼性を持つ必要がある)。

試験所が認可を受ける以前には、3GPP、O-RAN ALLIANCE、TIP、GSMA 等の組織は、現在は存在しないこうした基準の定義と公開を支援することができる。

2.7. 継続的改善

認証制度は、以前に付与されたいかなる認証も静的なものとみなすべきではない。認証制度は、5G/xG のイノベーションに対応するために動的認証プロセスを採用すべきであり、Open RAN の仕様及び標準が発展するにつれて、これらの変更を反映するように認証を更新すべきである。さらに、認証は、Open RAN の標準と仕様、及び既存のネットワークで使用されるインターフェース間の安全な後方互換性を保証するように設計されるべきである。加えて、ロバスト性を保証するために、試験用機器の能力が向上するのに合わせ、テストプロトコルを更新すべきである。

3. 費用対効果の高い導入

3.1. アクセシビリティ

オープン RAN 認証は、あらゆる規模の企業が利用できるようにすべきであり、導入への障壁は最小限にすべきである。

[1] https://nukib.gov.cz/download/Prague_Proposals_on_Telecommunications_Supplier_Diversity.pdf

ネットワーク機器の認証のコスト構造は複雑であり、製造業者が主な責任を負い、多くの場合、エンドユーザーにコストを転嫁する。また、認証機関とテストラボも重要な役割を果たし、サービス料金を通じて収益を得ている。

各国政府は、国際的な基準の調和化を支援し、補助金や助成金を提供することで、これらのコストを最適化することができる。また、政府資金による試験施設の設置、官民パートナーシップの促進、試験方法の革新の促進は、さらにコストを削減することができる。これらの戦略は、より効率的で手頃な認証プロセスを生み出し、業界と消費者の両方に利益をもたらすことができる。

3.2. 自動化

Open RAN の認証においては、認証コストとエラーのリスクを低減するために、可能な範囲で最大限テストを自動化する必要がある。

3.3. 既存リソースの活用

Open RAN 認証制度では、新しいインフラストラクチャの開発を必要とするのではなく、専門的な認証試験所サービス等の既存のリソースを活用する方法を検討する必要がある。

3.4. 認証の仕組み

認証プログラムの開発には、認証に対する段階的アプローチの影響を考慮する必要がある。すべての階層は、単に認証の次のステップのための基準を設定するのではなく、意味があり、顧客の要求を刺激するものである必要がある。

異なる階層での Open RAN 認証を検討する場合は、異なる導入での多様なニーズと規模を考慮することが重要である。大規模な MNO の要件は、小規模なプライベート配置の要件とは大幅に異なる。例えば、大規模な Open RAN の導入では、ネットワークの効率性とベンダーの多様性に重点が置かれるが、（例えば、鉱業や農業分野の）プライベートネットワークでは、信頼性とリアルタイムの監視が重視される。ニュートラルホストネットワーク、遠隔地域の農村地帯への導入、あるいは公共の安全に関する適用は、多様なユースケースをサポートする Open RAN の汎用性をさらに実証する。Open RAN 認証の潜在的な（及び非網羅的な）階層の構造としては、次のようなものがありうる。

1. プライベートネットワーク層

- **スコープ：**
  小規模企業、リモート施設、ローカライズされたプライベートネットワーク等での小規模な導入。通常はシンプルさとコスト効率に重点が置かれているが、外来診療のように規模が限られていても高いセキュリティが必要なニッチなケースにも対応できる。
- **技術的要件：**
  - 基本的な機能テストにより、コアとなる運用標準と信頼性の高い接続性を確保する。

- 共通の Open RAN コンポーネント及びインターフェースとの相互運用性により、複数ベンダーの機器をシームレスに統合できる。
- 標準的なユースケースにおける一般的な脆弱性から保護するためのベースラインのセキュリティコンプライアンス。また、導入規模が限られていても、導入に際して機密性の高い運用が必要な場合には、カスタマイズされた一般的なセキュリティ対策（エンドツーエンドの暗号化、高度な脅威検出等）を含めることができる。
- シンプル化された導入及び管理機能

2.エンタープライズネットワーク層

- **スコープ：**
  地域のサービス・プロバイダ、特定の業界・大企業等での中規模の導入
- **技術的要件：**
  - 幅広い運用機能にわたって機能テストを強化
  - さまざまな Open RAN コンポーネント及びシステムとの高度な相互運用性
  - 高度な脅威検出及び軽減機能を備えた高度なセキュリティ対策
  - 一般的なワークロード下で信頼性の高い運用を確保するためのパフォーマンス・メトリック
  - 中程度の拡張性により、中間レベルのユーザー数とデバイス数に対応できる。

3.キャリアネットワーク層

- **スコープ：**
  さまざまな導入事例(農村部マクロ、都市部のニュートラルホスト、mMIMO 等)をカバーする、MNO 及びグローバル・サービス・プロバイダ向けの大規模な導入。
- **技術的要件：**
  - エッジケースを含むすべての運用面を網羅した包括的な機能テスト
  - 広範な Open RAN エコシステム及びレガシーシステム間の完全な相互運用性
  - 厳しい基準とベストプラクティスを満たす高度なセキュリティプロトコル
  - 多様で厳しい運用条件下での厳格なパフォーマンスと信頼性のテスト
  - 柔軟な導入オプションを備えた、多数のユーザーとデバイスをサポートする高い拡張性
  - 関連するすべての規格及び要件に関する規制の遵守

この構造は、サプライヤーと MNO の両方に利益をもたらし得る。小規模なサプライヤーは、まず基本的な要件を満たし、その強みやビジネス上の優先順位に基づき、徐々に高度なモジュールを追求することで、より容易に市場に参入することができる。試験と認証がより簡単な小規模な導入は、より高いコストにつながる広範な技術的な試験を必要とする大規模な導入と比較して、より低

いコストになる。このアプローチは、サプライヤーの能力に関する詳細な洞察を提供し、ネットワークのニーズに最も合致した特定の要件を満たす製品とソリューションを提供するベンダーを選択できるようにすることで、MNO を支援する。このプログラムは、Open RAN 技術の進化に合わせて、新しいモジュールを追加することによっても拡張できる。

3.5. 認証の範囲

認証制度の構造と合わせて、制度の範囲は、市場の最も広範なセグメントとの関連性を促進するように、かつそれでもなお意味があるものとなるよう調整されるべきである。認証制度は、実際の需要がほとんどなく、明らかに価値減となるような形に専門化されるべきではない。

さらに、Open RAN 認証の範囲は、評価されるインターフェース（例えば、フロントホールとミッドホール等）または機能（RU/CU/DU の組み合わせ）が、認証のユースケースで定義されるように、標準に準拠し、シームレスに機能し、他のネットワーク要素とスムーズに統合されることを保証する必要がある。この適応性のあるスコープは、異なる展開スケールにわたって、堅牢なパフォーマンス、セキュリティ、及び相互運用性を保証する。

3.6. 再認証

オープン RAN システムは非常に複雑になる可能性があり、ソフトウェア、計算ハードウェアまたはファームウェアの更新の再認証が必要になる場合がある。特に主だった更新に関しては、産業界は、このような再認証が迅速かつ有意義で、費用対効果の高いものであることを確保するために、必要な措置を講じる必要がある。関連する再認証は、標準の発展、特定の使用例、規制へのコンプライアンス、業界のベスト・プラクティス、リスク評価、ステークホルダーからのフィードバック、履歴データ、導入の技術的及び運用上のコンテキスト等の基準に基づいて決定する必要がある。このアプローチにより、不必要な冗長性、過剰な試験や認証なしに、重要な側面を確実にテストできる。

4. 採用の促進

4.1. 顧客の需要

Open RAN 認証制度は、MNO、その他のネットワーク構築者、及び無線インターネットサービスプロバイダやプライベートネットワークの顧客等のユーザーが、調達プロセスにおいてこの認証を必要とする場合にのみ、成功することができる。認証制度は、以下のように、顧客にとっての重要な価値の源泉を強調することを検討する必要がある。

- この認証制度が、一層の革新をもたらし、業務の効率化をもたらすことができる強固で競争力のある市場を刺激する手段を提供することを強調する。
- Open RAN の構成要素が相互運用性、適合性、及びパフォーマンスの要件を満たすことを保証することで、認証によって導入リスクを最小限に抑

える方法を示す。互換性の問題を最小限に抑えることで、導入がスムーズとなり、ネットワークのダウンタイムが減少する。これは、運用者にとって重要なメリットである。

- この認証プログラムによって、進化する Open RAN テクノロジーと標準に合わせて柔軟に対応できることを強調し、運用者が将来にわたって利用できるネットワークを構築できるようにする。
- 実証済みの Open RAN ソリューションの導入が成功したことを示す機会を運用者に提供する。導入事例や事例紹介が貴重な実例となり、他の運用者がそれに従うよう促すことができる。

4.2. 産業界による支援

認証プログラムは、Open RAN 市場のサプライヤーの間で支持基盤を構築し、管轄区域間での断片化を避ける必要がある。これは、小規模事業者にとって市場参入を困難にする可能性があるためである。

認証プログラムは、産業界からの参加者にとって支援的な環境を発展させることを含め、幅広いサプライヤーを惹きつけ、維持するように設計されるべきである。

- **一貫性の促進：** 認証基準、プロセス、ガイダンスのための公開されたプラットフォームを開発し、透明性を確保し、異なる地域間の細分化を低減する。確立されたグローバルスタンダードを活用して、信頼を育み、国際的なベストプラクティスと整合性のある認証枠組みを構築する。
- **認証プロセスの最適化：** さまざまな規模や機能の導入に対応するために、モジュラー型または階層型の枠組み等、コスト効率性に優れた柔軟な認証戦略を採用する。
- **協力と知識交換の促進：** 業界全体のフォーラム、ワークショップ、及び研修会を組織して、ベストプラクティスの共有を促進し、認証ガイダンスを提供する。
- **認証登録の確立:** すべての認証されたサプライヤーとその能力を記録し、公的にアクセス可能な認定データベースを作成し、維持する。これにより、参加者に対して透明で公平な競争条件が確保される。
- **詳細な認証情報の提供：** 単純な合否判定形式の結果を超えて、製品の強みや KPI に関する洞察の提供に焦点を当てた包括的なレポートを含めることで、認証プログラムを変革する。

4.3. 政府による支援

各国政府は、Open RAN 認証制度の導入を促進する上で重要な役割を果たすことができる。各国政府は、それぞれの国固有の状況と優先順位を考慮した上で、複数のアプローチを検討することを検討することができる。そのための段階として、以下が考えられる。

- 適切な枠組みにおいて、公共調達の要件として、認証の取得が必要かどうかを検討すること(ただし、政府は独自の Open RAN 認証プログラムを開発したり運営したりすることを避けるべきである)。
- Open RAN 認証の取組者に対し、税制上のインセンティブ、助成金、またはその他の資金提供プログラムを提供する。これには、小規模 MNO 及びサプライヤーの参加を支援することを目的としたものも含まれる。
- 国際的なパートナーと協力して、Open RAN の導入を推進するための R&D ブレイクスルー、パイロットプログラム、ベストプラクティス、キャパシティビルディング、規制措置等の経験を共有する。
- 産業界と連携して、世界的なキャパシティビルディング、一般教育、及び人材育成の取組を支援するために国際的なパートナーと調整し、Open RAN ソリューションをグローバルにテスト、開発、統合するために必要な人材へのアクセスを確保する。

5. 結論

堅牢な Open RAN の採用を推進するために、ステークホルダーは、相互運用性、適合性、パフォーマンス及びセキュリティを保証する包括的な認証枠組みを確立し、維持する必要がある。RAN システムの複雑さの増大、MNO 間のリソースの制約、及びサプライヤーが製品の能力を実証する際に直面する困難は、そのようなフレームワークを開発することの意義を強調している。認証制度は、そのような障害を克服し、製品の完成度に対する顧客の信頼を提供し、より広範な導入を促進するための鍵である。この分野における既存の取組は有望なものである一方で、まだ初期段階にあり、これらの課題に効果的に対処するために進化しなければならない。

MNO、ベンダー、研究機関、政策立案者等の関連するステークホルダー間の協力は、応答性の高い認証の枠組みを形成するために極めて重要である。また、地域の試験所は、透明性のある検証プロセスを可能にし、供給者の負担を軽減する上で中心的な役割を果たすことができる。産業界が認証プログラムの開発を主導すべきである一方で、政策立案者は、補助金、税制優遇措置、迅速な規制承認等の取組を通じて、導入の奨励を検討することができる。また、公共調達への認証制度の適用は、採用を加速させる可能性もある。最後に、政策立案者は、地域産業のエコシステムやイノベーターを育成し、貿易障壁に取り組み、労働力開発の取組を支援することができる。

GCOT パートナーは、このようなアプローチの発展と長期的な耐久性と有用性を支援する上で、政府が果たすべき役割があると考えている。GCOT パートナーは、英国の SONIC (SmartRAN Open Network Interoperability Center) Labs や米国の CRAIN (Communications Research and Innovation Network) のような中立的な研究所の設立や、「Public Wireless Supply Chain Innovation Fund」

のような研究開発基金、及び「Open Network Ecosystem Competition」のようなコンテストを通じたOpen RANエコシステムへの政府投資を通じて、この原則を支持しており、今後も引き続き支持をする。GCOT のパートナーは、追加的な政府の支援と関与を歓迎する。GCOTパートナーは、引き続き産業界主導のOpen RAN アプローチへの移行を支援し、この方向への重要なステップとして、認証枠組みの開発においてステークホルダーと建設的に関与する。