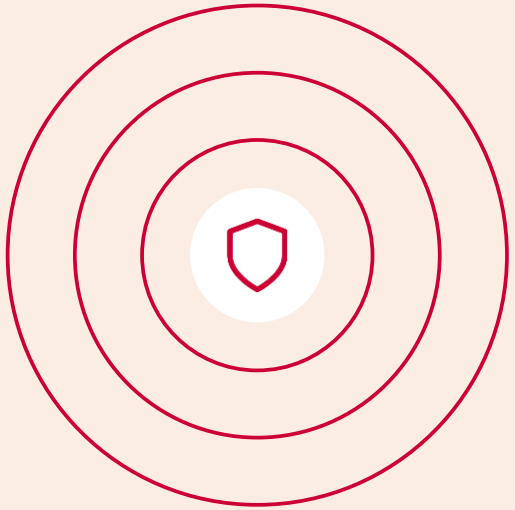
A Proposal for Hybrid Use of PQC and QKD

～ MPLS JAPAN 2026 ～

2026年10月26日

NTTドコモビジネス株式会社
イノベーションセンター 技術戦略部門/IOWN推進室
耐量子暗号エバンジェリスト

森岡　康高



CHALLENGES

量子コンピュータ時代を見据えた量子暗号(QKD)とPQCの課題

QKD 課題

- **機能の制約**

QKDのデバイス間で安全に鍵を共有するのみ
認証機能が無い

- **コスト**

QKDデバイスやTrusted Nodeなど, 特別なハードウェアによるコストの増大

- **Trusted Node**

物理距離の制限を突破するために利用する鍵リレーにおいて,
鍵データが露出するため, Trusted Nodeを想定

PQC 課題

- **計算量的安全性**

PQCも古典暗号と同様に，将来的に危殆化する可能性がある

- **信頼性**

PQCアルゴリズムは, 比較的新しい数学理論を用いており,
実システムの利用実績が乏しい

- **運用**

PQCアルゴリズムを実装した実システムの運用実績が少ない

APPROACH

提案アーキテクチャにおける対応

解決策

KEMなどにより共有した鍵を用いた, Wegman-Carter MACによる認証機能付加

— 機能の制約

PQCによる保護領域(key establishment / distribution plane)とQKDによる保護領域(Key application plane)の分離

— 計算量的安全性

解決策

特別なハードウェアを利用しない CV-QKDの活用

— コスト

古典暗号を含め, 複数PQCアルゴリズムによるハイブリッド鍵導出 (Multi Factor Security)

— 信頼性

解決策

Confidential Computingの活用 (IOWN* PETs + 暗号化)

— Trusted Node

key establishment / distribution Plainのクラウド化

— 運用

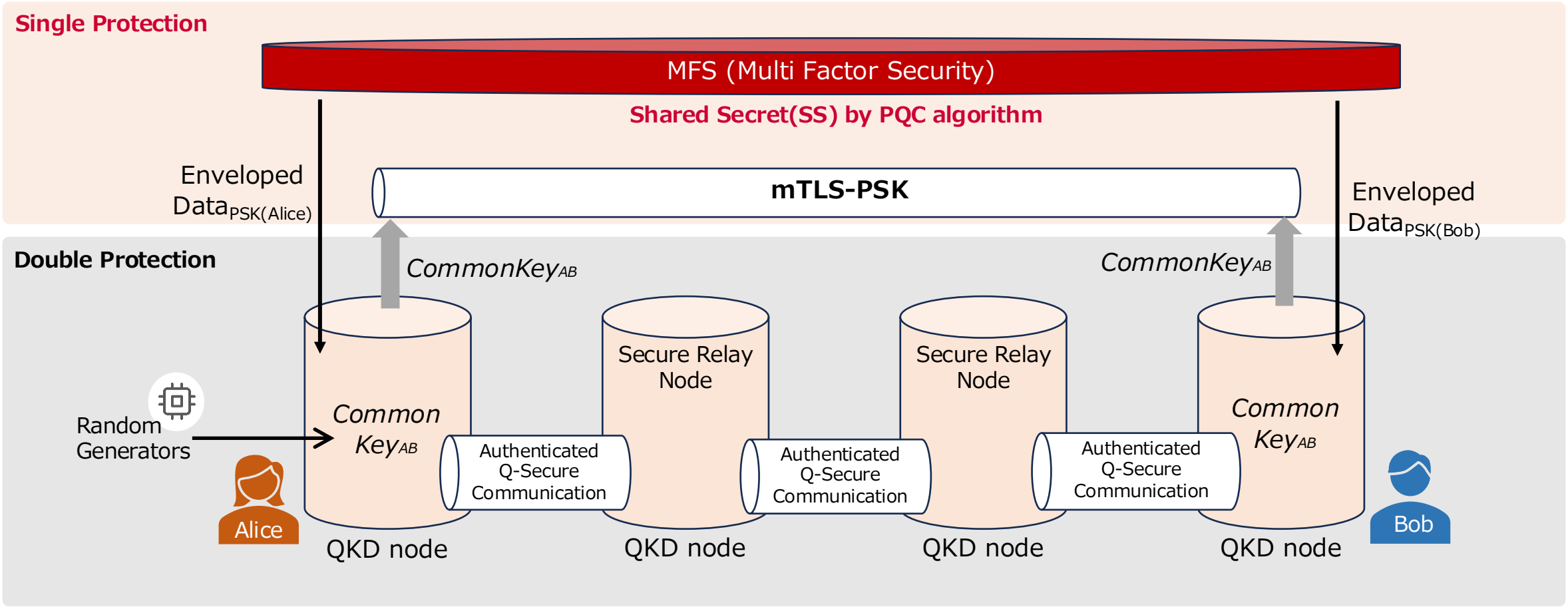
*IOWN (Innovative Optical and Wireless Network): A next-generation infrastructure initiative featuring all-photonics networking for high-capacity, low-latency, and energy-efficient digital services.

**MFS (Multi-Factor Security): Enables crypto agility by combining multiple cryptographic technologies for resilient quantum-safe communications.

ARCHITECTURE

QKD/PQC Hybrid Architecture

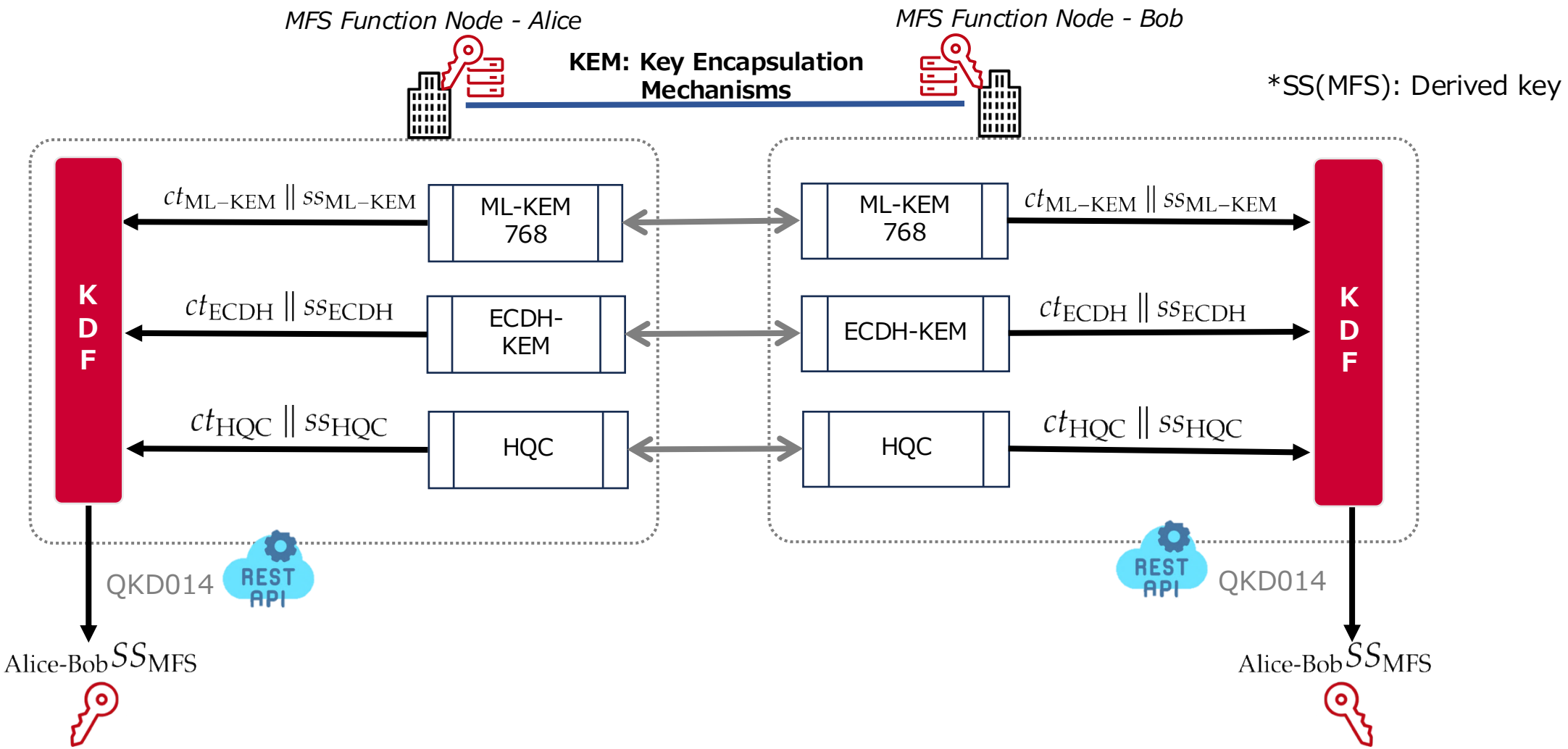
PQCのみのSingle Protectionと，PQC+QKDのDouble Protectionで保護領域を分離したアーキテクチャ



ARCHITECTURE

Key Establishment / Distribution Plane by MFS Cloud

クラウド上で, key establishmentのクリプト・アジリティ確保

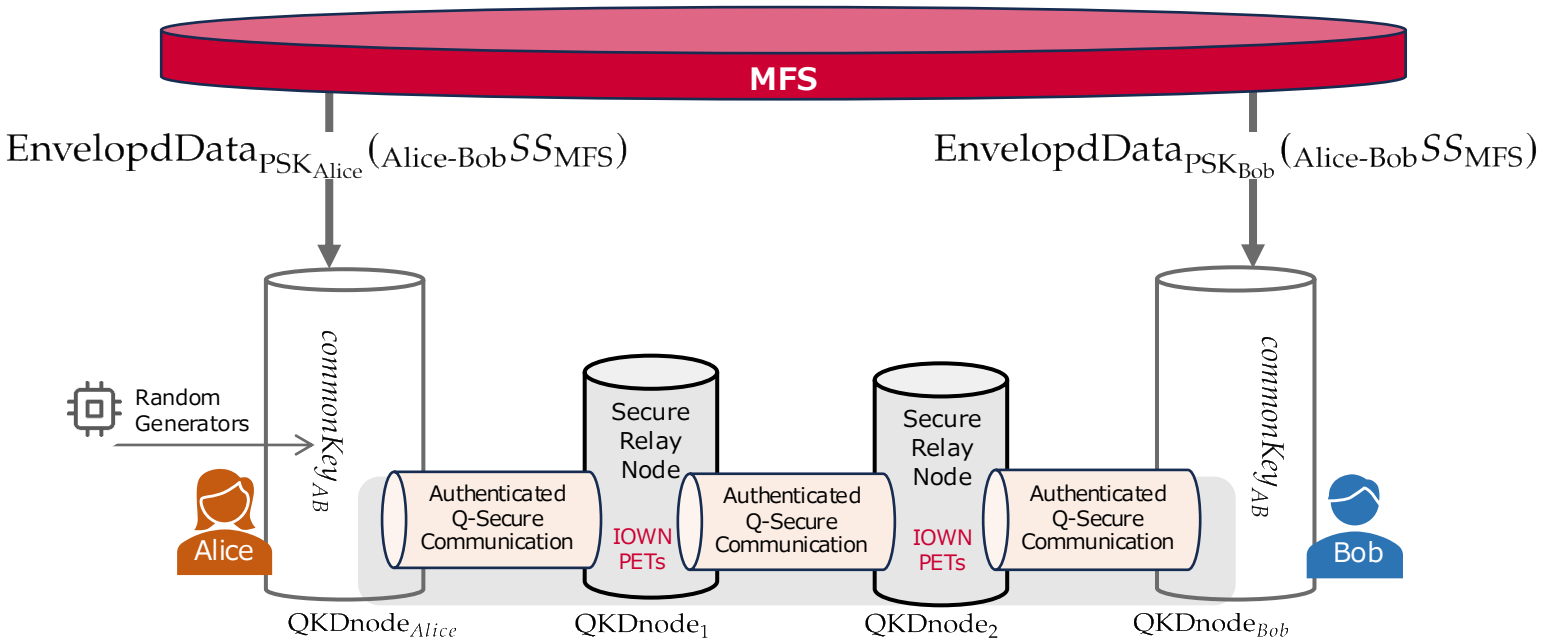


MECHANISM

Confidential Computing at Trusted Nodes

Trusted Nodeにおいてもデータを暗号化したまま、安全な中継処理を実現

- IOWN PETs（TEE）を用いて, 安全な中継ノードを構築
- データは, 中継処理の全過程を通じて暗号化された状態のまま転送



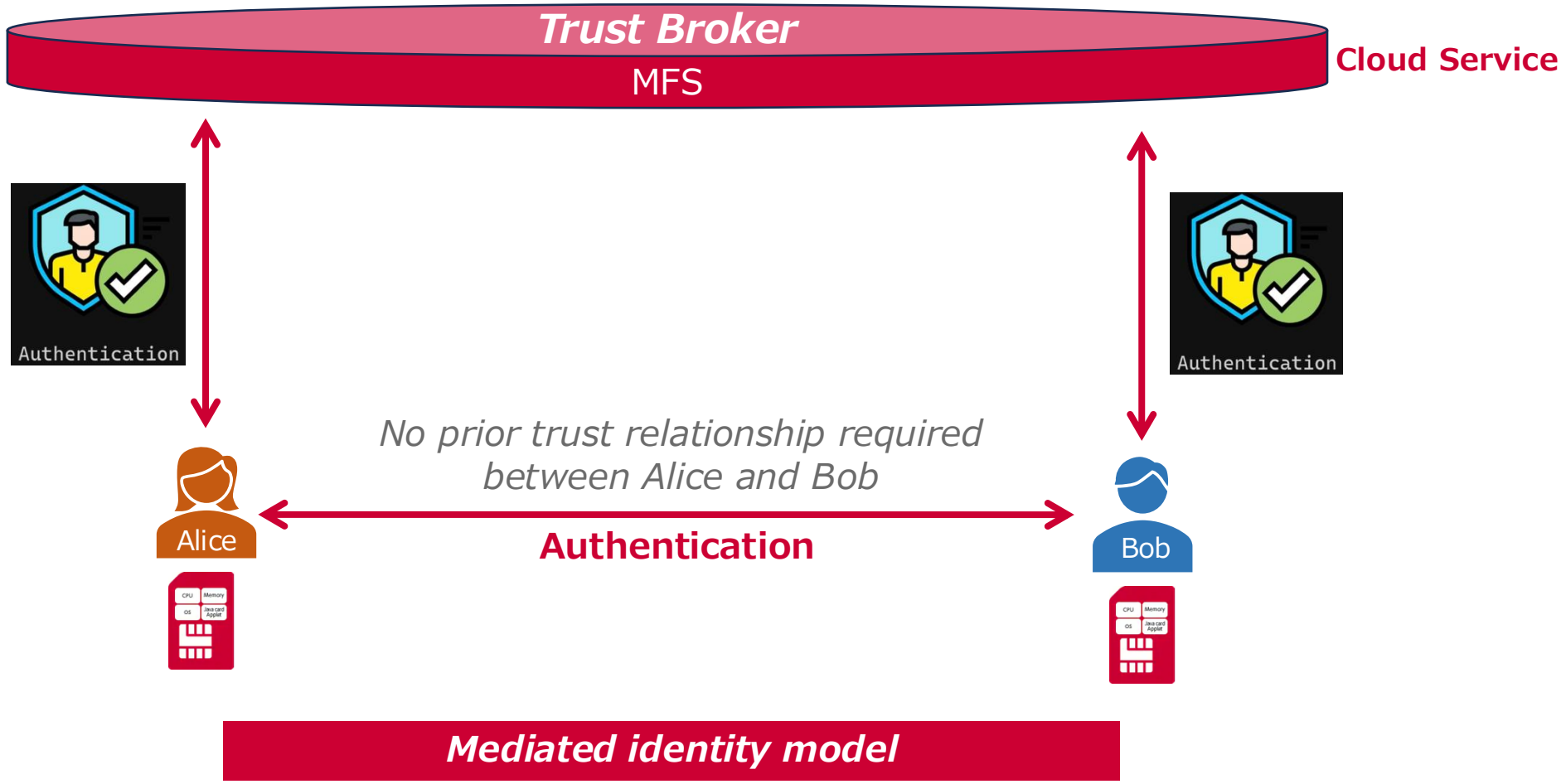
Benefits

- **物理セキュリティ要件の緩和**
- **Trusted Nodesのコスト低減**
- **CV-QKD導入のハードルを低減**

MECHANISM

Trust Broker by Cloud Service with wcMAC in SIM Applet

without Client Certificates



USE CASE

Use Case: Communication During Disasters

Without this system

- 初対面同士では, 安全に通信が出来ない
- PKI構築が必要
- 証明書発行が, 必要

With this system

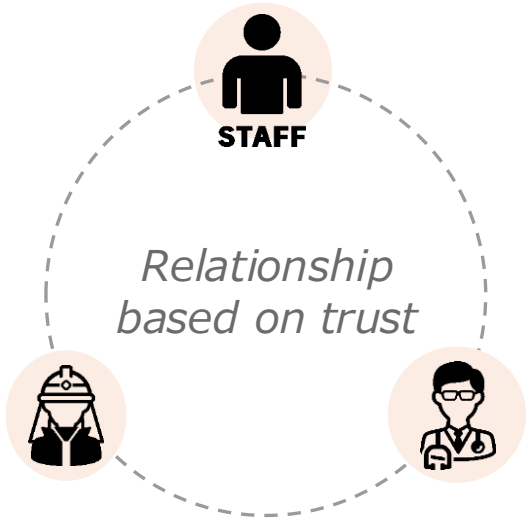
- SIMを利用し, 相互認証を実行
- Trust Brokerが, 信頼を仲介
- 証明書発行不要で, すぐにグループ通信を開設

Participants (example)

– Municipal government officials
– Fire department
– Police
– Medical institutions
– Evacuation shelter managers

Capabilities enabled via Trust Broker

– Mutual authentication
– Authorization
– Key sharing

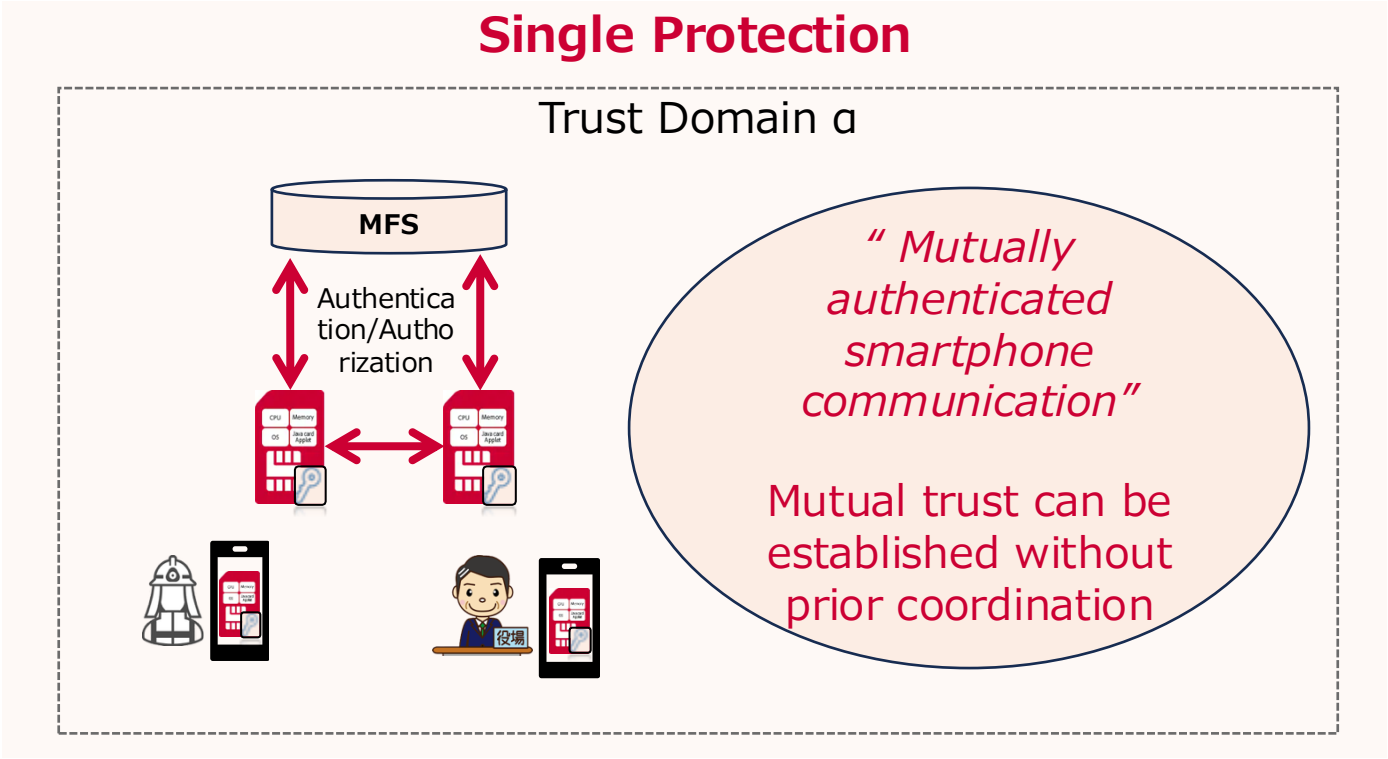


“ Even when meeting for the first time, as long as they have a SIM, they can communicate securely.”

USE CASE 1

Use Case 1: Single-Trusted Domain

SIM Use Case (Single Protection: 社会実装の初期モデル) — Pre-placed PSK in SIM enables mutual trust between smartphones without prior coordination.

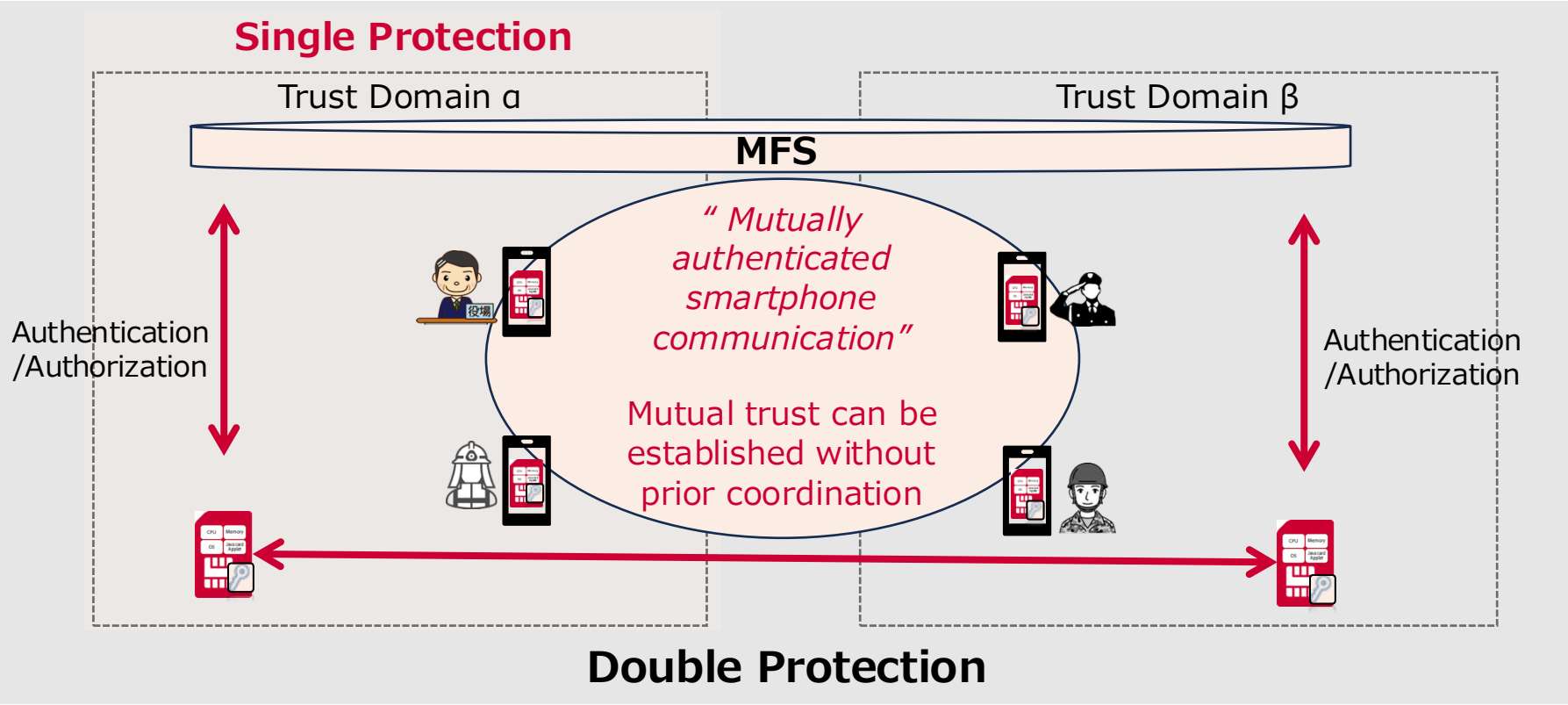


Single Protectionによって導入障壁を低減し，普及拡大を目指す

USE CASE 2

Use Case 2: Multi-Trusted Domain

SIM Use Case (Double Protection: 組織間連携モデル) — mutual trust across domains without prior coordination.



Double protectionにより, 将来的に安定したIdentity Mediation Infrastructure

CONCLUSION

Conclusion & Future Work

1

SIMをTrust Anchor とし，事前PKI関係を不要としたエンドポイント間相互認証

2

異なるDomain間に，量子暗号通信によるDouble protectionを適用

3

PQC，QKD，SIM認証，Trusted Nodeを「段階的に社会実装」

Roadmap — Future Work

① クラウドを用いたkey establishment / distribution plane分離によるCrypt agilityを確保

② Single/Double protection を使い分け，Dual-use による初期コスト抑制

③ Certificate-less なエンドポイント（SIM）相互認証

④ モバイルインフラを活用したSIM運用

⑤ Trusted Node ＋ CV-QKD によるコストの低減と専用ダークファイバの削減

⑥ CV-QKDを用いたテストベッドを構築中

つなごう。驚きを。幸せを。

NTT docomo Business