Intel SGXにおける2つのリモートアテステーションの利点と欠点の考察

矢川嵩*†, 照屋唯紀†, 須崎有康†, 阿部洋丈*

* 筑波大学　† 産業技術総合研究所

リモートアテステーションの利点

IoTやクラウドの普及に伴い遠隔管理の機会が増加

想定している相手か？
正常に稼働しているか？

リモートアテステーション(RA)

プラットフォーム及びその上で動作しているソフトウェアの真正性を検証によって遠隔で確認できる仕組み

Intel SGXのリモートアテステーション

Intel Software Guard Extensions(SGX)
ソフトウェア保護機能を持ったCPU拡張であり、
2種類のRAに対応している

EPID Attestation
プライバシー保護に配慮

ECDSA Attestation
サードパーティを利用してのRAが可能

2つを比較した時の利点と欠点は不明瞭

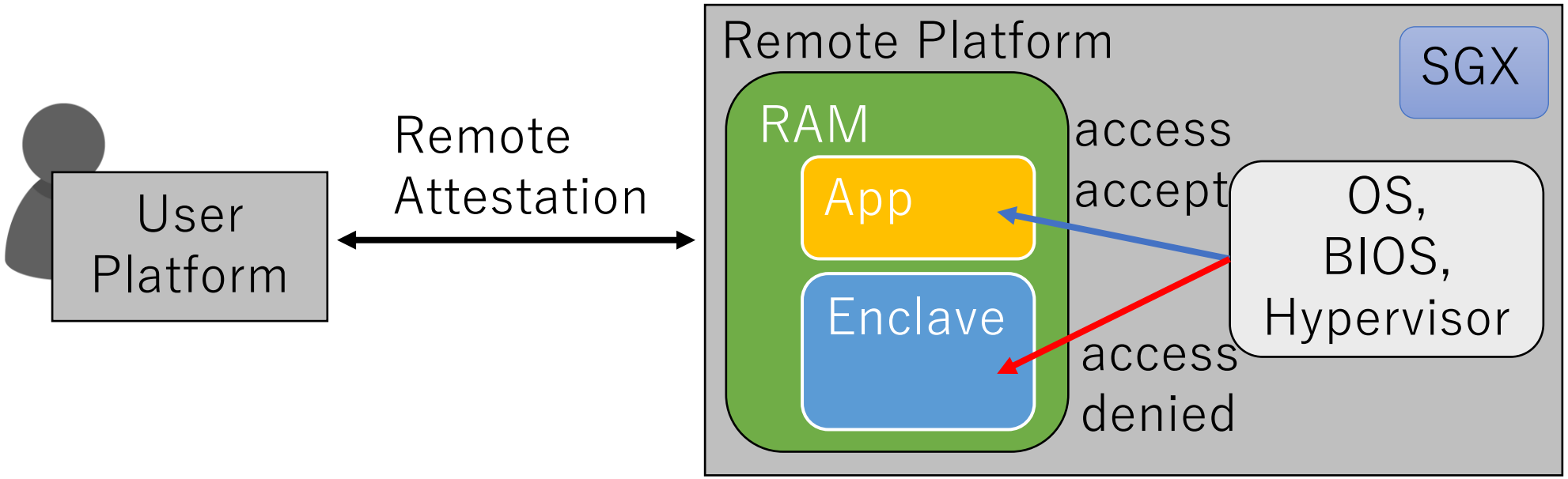
→ **仕様や性能の比較によって利点と欠点を明らかにする**

目次

- 背景知識
  - Intel SGX
  - リモートアテステーション
- 2つのリモートアテステーションについての比較
  - 仕様や実装の差
  - 性能の差
- 利点と欠点の考察
- まとめ

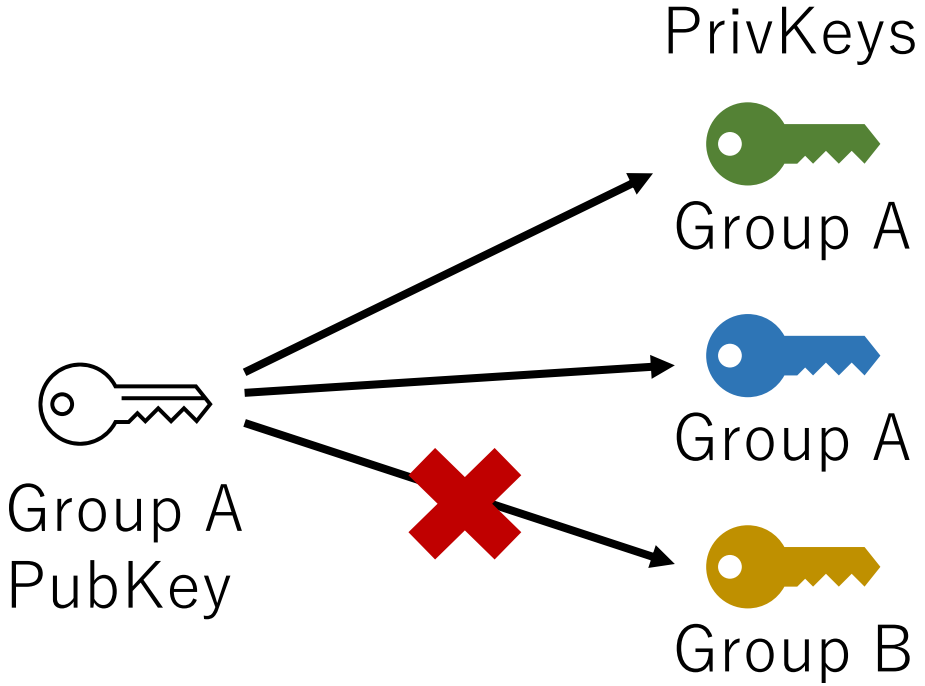
Intel SGX

- CPU内のHW鍵を利用してメモリを暗号化し、OSやハイパーバイザ等からの特権的な攻撃からも保護する
- 暗号化領域はEnclaveと呼ばれ、改ざん検証もされる
- RAではプラットフォームと対象のEnclaveの真正性を確認



EPID Attestation[1]

- EPIDは公開鍵と秘密鍵の対応が 1 対 N
  ＝ グループ公開鍵とメンバー秘密鍵が対応
- 検証時に利用者を特定することはできない
- グループはSGXの
  TCB(バージョン情報)と
  CPUタイプ(e.g., Core i5)
  の組み合わせで分けられる



[1] Simon Johnson et al. Intel software guard extensions: EPID provisioning and attestation services, Mar. 2016.

ECDSA Attestation[2]

- Intel 以外の第三者が作成した検証サービスの利用が可能で、検証内容の拡張が可能
- 匿名性が不都合な場合やIntel の検証を信頼しない場合、大規模なイントラネットを持つデーターセンターなどを想定
- Intel SGX Data Center Attestation Primitives (DCAP)を使用することで利用環境を構築できる
- DCAPはライブラリや特殊なEnclaveなどを含むパッケージであり、ローカル環境で構築可能な検証サービスも含む

[2] Simon Johnson et al. Supporting third party attestation for Intel SGX with Intel data center attestation primitives, 2018.

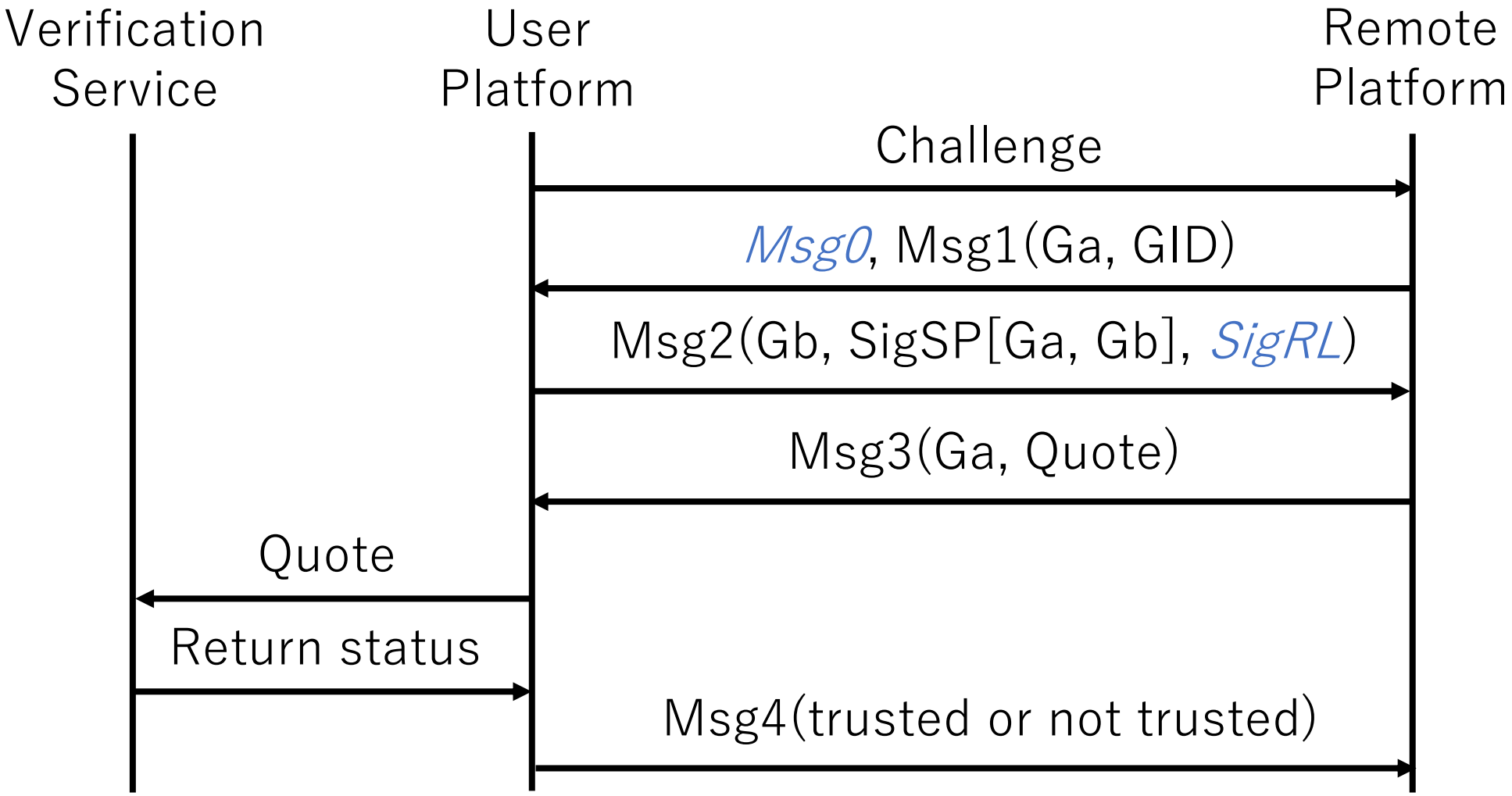
リモートアテステーションのプロトコル

- DH鍵共有に対象のEnclaveとプラットフォーム情報の検証を含んだ独自のもの
- 特定のメッセージ(Msg0~4)のやり取りによって完了する
- 検証に必要な情報はまとめてQuoteと呼ばれ、CPU、Enclaveについてのバージョン情報等が含まれる
- Quoteの検証はユーザー側が専用の検証サービスを利用することで行う

メッセージ

メッセージ	方向	内容
Msg0 (EPIDのみ)	From Remote	• 拡張EPIDグループID
Msg1	From Remote	• DH鍵共有用の公開鍵(Ga) • EPID グループID(GID)
Msg2	To Remote	• DH鍵共有用の公開鍵(Gb) • GaとGbを関連付ける署名(SigSP[Ga, Gb]) • 署名失効リスト(SigRL)(EPIDのみ)
Msg3	From Remote	• Ga • Quote
Msg4	To Remote	• 信頼するか否か(フォーマット自由)

プロトコルフロー

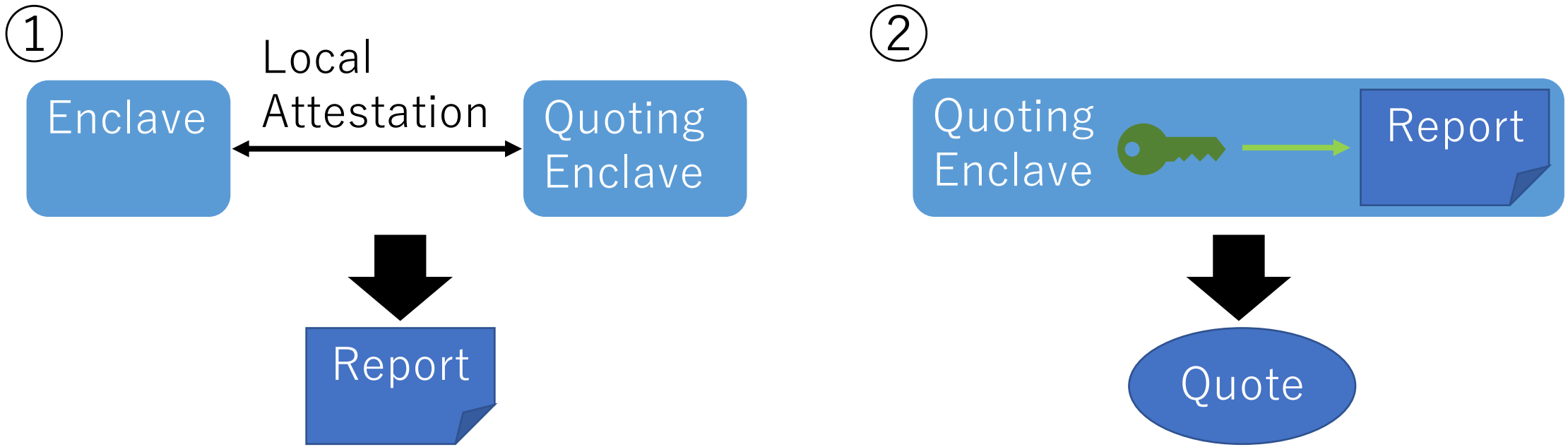

Verification Service
User Platform
Remote Platform
Challenge
Msg0, Msg1(Ga, GID)
Msg2(Gb, SigSP[Ga, Gb], SigRL)
Msg3(Ga, Quote)
Quote
Return status
Msg4(trusted or not trusted)

Quoteの生成

- Quoting Enclave(QE)：Quote生成のための特殊なEnclave

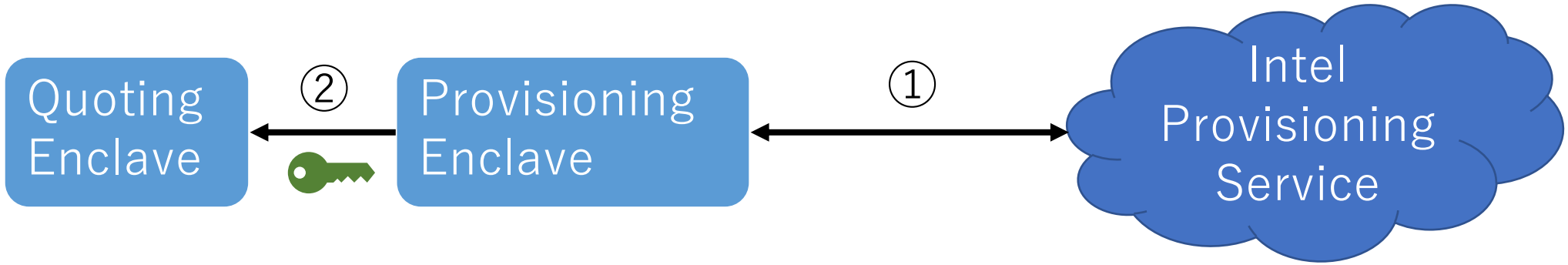
①Local Attestation：QEと対象Enclaveとの相互検証

②QE内のAttestation Key(プラットフォームとそのTCBに固有の非対称鍵)でReportに署名



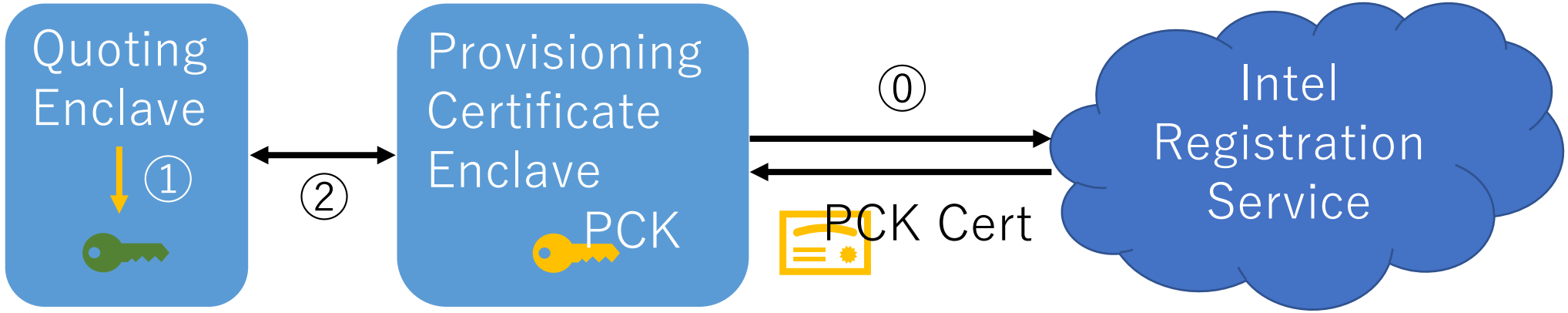
Attestation Keyのプロビジョニング(EPID)

- Attestation KeyはEPIDメンバー秘密鍵
- Provisioning Enclave(PvE)とIntel Provisioning Serviceとの通信によってグループ決めを含むプロビジョニング(①)を行い、その後Attestation KeyはQEに渡される(②)
- PvEはCPUに固有の鍵であるProvisioning Key(PK)を利用
  - PKはIntelも生成でき、PvEの真正性確認に利用



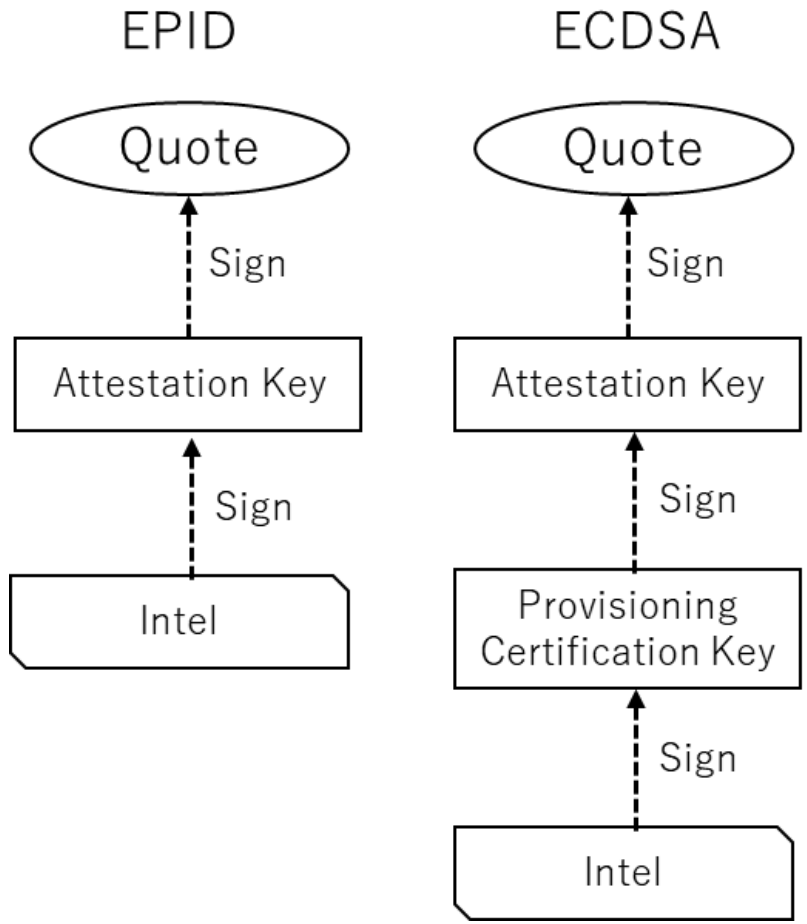
Attestation Keyのプロビジョニング(ECDSA)

- Attestation KeyはECDSA
- Attestation KeyはQE内で生成(①)された後、 PCE内のProvisioning Certification Key(PCK)で署名される(②)
- 予めIntel Registration Serviceにプラットフォームとそのの TCBについての情報を登録する事で、PCK証明書が発行される(⓪)



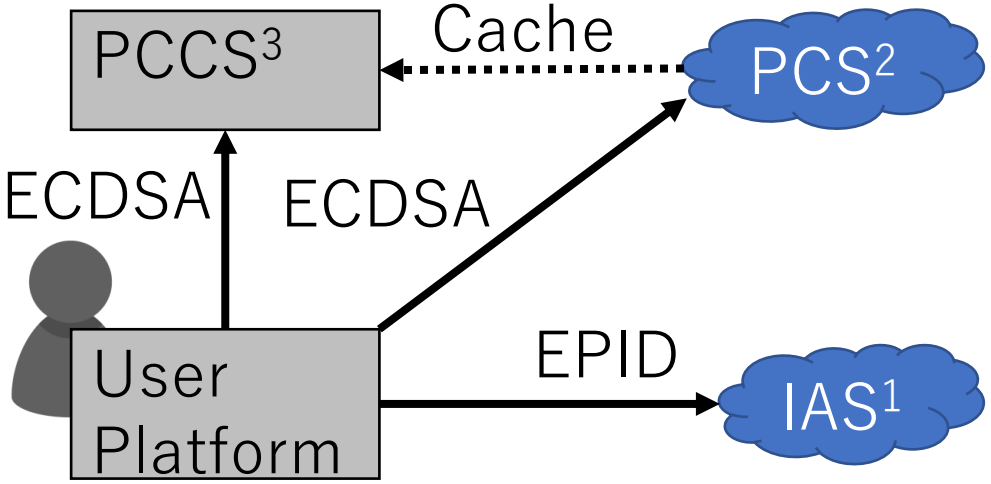
Quoteの検証

- EPID Attestation：適切なEPIDグループ公開鍵による署名の復号
- ECDSA Attestation：署名の鎖
- 検証内容：署名が正しいか、各種失効リストに該当していないか等
- ECDSA AttestationではEnclaveの情報が想定と同様かどうかの検証も義務付けられている(EPIDでは任意)



検証サービス

- EPID Attestation：オンラインサービス(IAS)でのみ検証可能
- ECDSA Attestation：オンラインサービス(PCS)の他に、ローカル環境に構築された検証サービス(PCCS)も利用可能
- PCCSには予め適切なPCK証明書をPCSからキャッシュしておく必要がある



1. Intel Attestation Service(IAS)
2. Intel Provisioning Certification Service(PCS)
3. Intel Provisioning Certificate Caching Service(PCCS)

特殊なEnclave

種類	名称	用途	実装
EPID Attestation	Launch Enclave	PvEとQE(HW)の起動	HW
	PvE	Attestation Keyのプロビジョニング	
	QE	Quoteの生成(EPID)	
ECDSA Attestation	Reference Launch Enclave	PCEとQE(SW)の起動 (Intel以外の署名付Enclaveの起動)	
	PCE	QEのローカル認証局の役割	SW (DCAP)
	QE	Quoteの生成(ECDSA)	
	Quote Verification Enclave	Quoteの検証 (検証用プラットフォームで使用)	

拡張性

- Microsoft Azure[3]では、ECDSA Attestationについては専用プラグインがあり、Azureが提供するIntelからのキャッシュ情報を利用できる
- SCONE[4]はコンテナ保護機構であり、秘密管理を一任できるConfiguration and Attestation Service(CAS)が利用できる。
  CASではSCONEで扱うEnclaveに対するリモートアテステーションについての一括設定も可能であるが、独自の拡張は現在ない

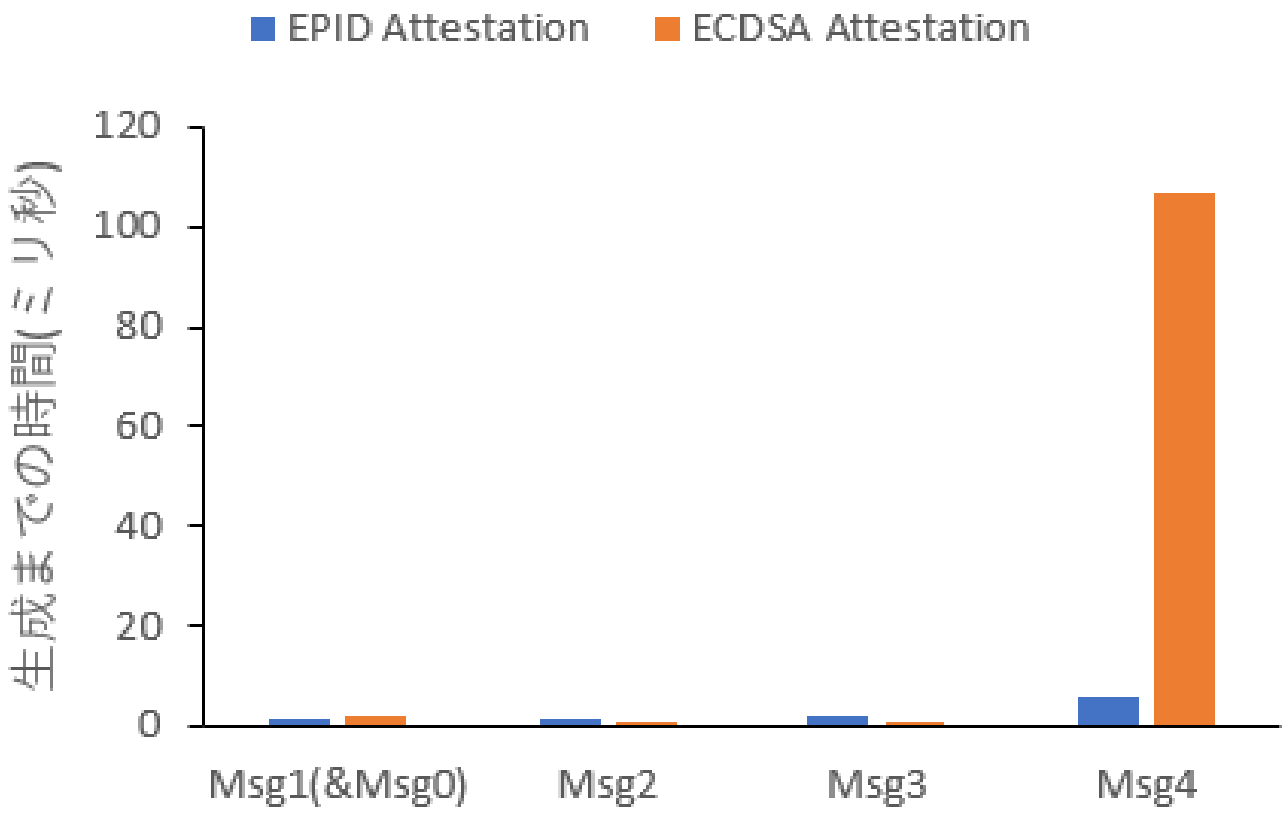
[3] Microsoft Azure, Jan. 2022. https://azure.microsoft.com/.

[4] Sergei Arnautov et al. SCONE: secure Linux containers with Intel SGX. In Kimberly Keeton and Timothy Roscoe, editors, OSDI 2016, Savannah, GA, USA, November 2-4, 2016, pp.689–703. USENIX Association, Nov. 2016.

各メッセージの生成時間

- ECDSA Attestationではローカル環境で検証
- Msg1, Msg2, Msg3の生成時間の差は2ms以内
- Msg4は約18倍の差

検証内容の差



安全性についての考察

項目	考察
鍵の保護	• Root of TrustはどちらもCPU内のHW鍵 • 各種鍵は各Enclave内で適切に保護される
失効リスト	• IASでは常に最新版が適用される • PCCSでは更新については任意のため注意が必要
検証内容	• EPID Attestationではユーザー側で確認しない場合、同一プラットフォーム上のEnclaveとすり替えができる可能性有
プライバシー	• EPID Attestationでは鍵によってプラットフォームは特定されず、署名失効による間接的な鍵の失効に対応 • ECDSA Attestationに匿名性は無いが、検証時にIntelに接続しないため、IPアドレス等の情報はIntelに渡らない

利便性についての考察

項目	考察
実行時間	• EPID AttestationではIASの利用が不可欠なため、ネットワーク環境が悪い場合には実行時間が遅くなる可能性がある • ECDSA AttestationのQuote検証は遅いが、どのような操作によって遅くなっているかの解析は今後の課題である
拡張性	• EPID Attestationでは検証サービスがIASのみのため拡張性は低くなる • ECDSA Attestationでは第三者が構築した検証サービスを利用できるが、信頼できるサービスを見極める必要がある

まとめ

- Intel SGXの2種類のリモートアテステーションについて比較を行い、それらの利点と欠点について考察した。
- EPID Attestationはプライバシー保護に注力しているが、その分拡張性は低く、Intelへの依存度も高い
- ECDSA Attestationは拡張性は高いが、第三者がある程度自由に設定を行えるため注意が必要
- ECDSA Attestationでの検証における具体的な操作についての調査は今後の課題である