Intel SGX における 2 つのリモートアテステーションの比較

矢川嵩[1, 2]　照屋唯紀[2]　須崎有康[2]

1. はじめに

近年はクラウドや IoT の普及に伴い，デバイスの管理や操作を目的とした遠隔操作が増えている．この遠隔操作の際にリモートアテステーションを行う事により，ユーザーは遠隔でデバイスやデバイス上のソフトウェアの健全性を確認できる．Intel Software Guard Extensions(SGX)は，隔離実行環境である Enclave で信頼できるアプリケーションを実行する際に，複数のリモートアテステーションに対応している．本稿では，この Intel が提供する SGX のリモートアテステーションについて比較する．

2. Intel SGX

Intel SGX は，Intel 第 6 世代 CPU 以降で利用可能な CPU の拡張機能であり, Trusted Execution Environment(TEE)の一種である[1]．SGX で使用するメモリは起動時に通常の OS とは別に確保され, Memory Encryption Engine という特別なハードウェアによってメモリを暗号化することにより, OS やハイパーバイザ等を利用した特権的な攻撃からもデータやプログラムを保護することが出来る．この暗号化されたメモリ領域は Enclave と呼ばれ, 1 つのプラットフォームにつき複数個生成することができる．また, Enclave に入れるプログラム及びデータは開発者が自由に決めることが出来る．ただし，それらが信頼できるかどうかの判断は開発者の責任である．

SGX はリモートアテステーションに対応しており, ユーザーは遠隔の SGX 対応プラットフォームと Enclave 内のプログラム及びデータの健全性を確認できる．

SGX のリモートアテステーションのプロトコルは DH 鍵共有に対象の Enclave とプラットフォームの認証を含んだ独自のものである．この認証のためにユーザー側に渡される情報は構造体としてまとめられており，これは Quote と呼ばれている．Quote には，ハードウェア TCB，CPU，対象の Enclave についての情報が含まれており，これらを検証することによって遠隔プラットフォームの SGX が正常に動作していることを確認できる．Quote の生成手順は以下の通りである．

(1) 遠隔プラットフォーム上にある対象の Enclave と Quoting Enclave(QE)とで Enclave 間の認証を行うことで, Report と呼ばれる構造体を発行する．QE は，Quote を生成するための特殊な Enclave で，Intel によって署名されている．

(2) QE は QE 内に保存されている Attestation Key(AK)と呼ばれる署名鍵によって Report に署名することで Quote を生成する．

また，SGX のリモートアテステーションには，AK に Enhanced Privacy ID(EPID)[2][3]を利用するものと，ECDSA を利用するものの 2 つが存在する．

EPID は Direct anonymous attestation (DAA)[4]に署名鍵失効についての拡張を加えた暗号化アルゴリズムであり，これによりプラットフォームの匿名性を保ったままでのリモートアテステーションが可能となる. DAA では検証鍵と署名鍵の対応が 1 対 N になっているため，どのプラットフォームが生成した Quote か，2 つの Quote がある場合にそれが同一プラットフォームで生成されたものか判別することはできない．

ECDSA を利用したリモートアテステーションでは，サードパーティでの Quote の検証も可能である[5]．また，サードパーティでの認証をサポートするために，Intel は Intel SGX Data Center Attestation Primitives(DCAP)[6]と呼ばれるパッケージを提供している．DCAP は ECDSA のみをサポートし，プラットフォームの匿名性を強制する EPID では不都合なデータセンター等での利用を想定している．ECDSA を利用する場合は DCAP を用いる場合がほとんどであり，以降は本稿でも ECDSA を利用する場合は DCAP を利用しているものとする．

3. リモートアテステーションの比較

EPID の AK で署名された Quote は, Intel が提供する Intel Attestation Service(IAS)を利用してのみ検証できる. EPID の AK は Intel に署名されている．IAS では，EPID の AK に対応した検証鍵を用いることで Quote を検証する．これに対し，ECDSA の AK で署名された Quote は，Intel が提供する Intel Provisioning Certification Service(PCS)によって検証できる．ECDSA の AK は，Provisioning Certification Enclave(PCE)内に保存されている Provisioning Certification Key(PCK)によって署名されている．PCE は QE と同一プラットフォーム内にあり，QE のローカル認証局としての機能を持つ．また，PCK は Intel によって署名されている．図 1 に EPID と ECDSA それぞれの Quote に対する署名について示した．PCS では，対応する PCK 及び AK の署名を検証することによる信頼の鎖で Quote を検証する．また，ECDSA の場合，ローカル環境に構築した Provisioning

1 筑波大学
University of Tsukuba
2 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology

Certificate Caching Service(PCCS)でQuoteを検証することもできる．PCCSはDCAPに含まれており，PCKの証明書を保存しておくためのデータベースである．PCCSにプラットフォーム情報を登録すると，PCCSはそれに対応したPCK証明書をPCSから取得する．これにより，PCCSに登録したプラットフォームで生成したQuoteであれば，PCCSでそれを検証できるようになる．また，IASやPCSと異なり，PCCSの利用はオフライン環境であっても可能である．図2はEPIDとECDSAそれぞれのQuoteの生成と検証の流れについて示したものである．Challengerは Quote を Remote Platformから受け取った後，Quoteの検証のためにその署名に応じた適切なサービスを利用できる．

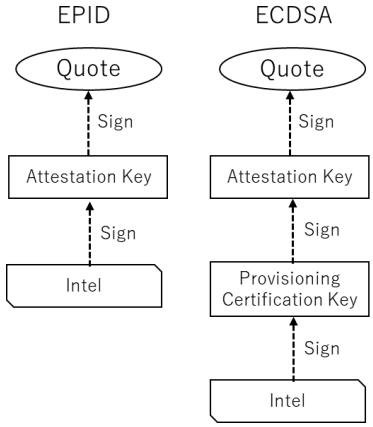

図 1 Quoteに対する署名

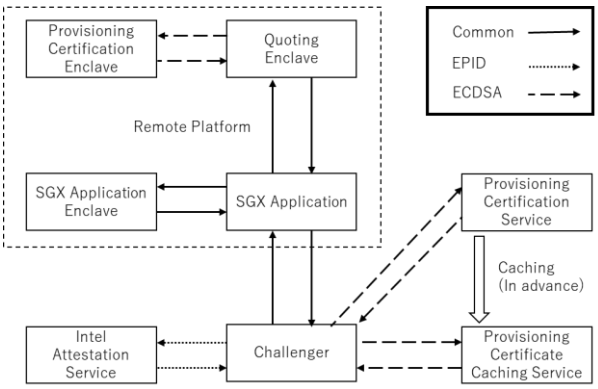

図 2 Quoteの生成と検証のフロー

リモートアテステーションの過程で利用される特殊なEnclaveも，EPIDとECDSAでは異なる．EPIDでは，QEの他にProvisioning Enclave(PvE)を利用する．PvEはIntelと通信することで，EPIDのAKを生成する．これらはハードウェアとして実装されており，Intelに署名されている．これに対してECDSAでは，QEとPCEの他にQuote Verification Enclave (QvE)を利用する．QvEはQEで生成されたQuoteを検証するためのものであり，これを利用するプラットフォームはSGXに対応していなくても良い．これらはソフトウェアとして実装されており，DCAPに含まれる．また，これらはIntelに署名されている．

4. おわりに

本稿では，Intel SGXにおける2つのリモートアテステーションについて比較を行った．現在もGithubで公開されているプログラムを追うなどして，各々の仕様について引き続き調査を進めている．また，今後はこの調査を元に，ECDSAを利用したリモートアテステーションの課題を解決する事を検討している．

参考文献

[1] 須崎 有康，Trusted Execution Environmentの実装とそれを支える技術，電子情報通信学会 基礎・境界ソサイエティ．Fundamentals Review，2020年14巻2号 p. 107-117
[2] Ernie Brickell，Jiangtao Li．Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities．WPES，October 2007, Alexandria Virginia，USA.
[3] Simon Johnson，Vinnie Scarlata，et al．Intel® Software Guard Extensions: EPID Provisioning and Attestation Services．INTELCORP，March 2016.
[4] Ernie Brickell，Jan Camenisch，Liqun Chen．Direct anonymous attestation．CCS，October 2004，Washington DC，USA.
[5] Simon Johnson，Vinnie Scarlata，et al．Supporting Third Party Attestation for Intel® SGX with Intel® Data Center Attestation Primitives．INTELCORP，2018.
[6] Muhammad Usama Sardar，Rasha Faqeh，Christof Fetzer．Formal Foundations for Intel SGX Data Center Attestation Primitives．ICFEM，March 2020.