A Privacy Friendly Method for Assuring Trust

Ernie Brickell

Intel Corporation

Agenda

- Problem Statement
- Existing solutions
- Direct Proof Protocol
  - Properties
  - Outline of protocol

Trusted Platform Module (TPM)

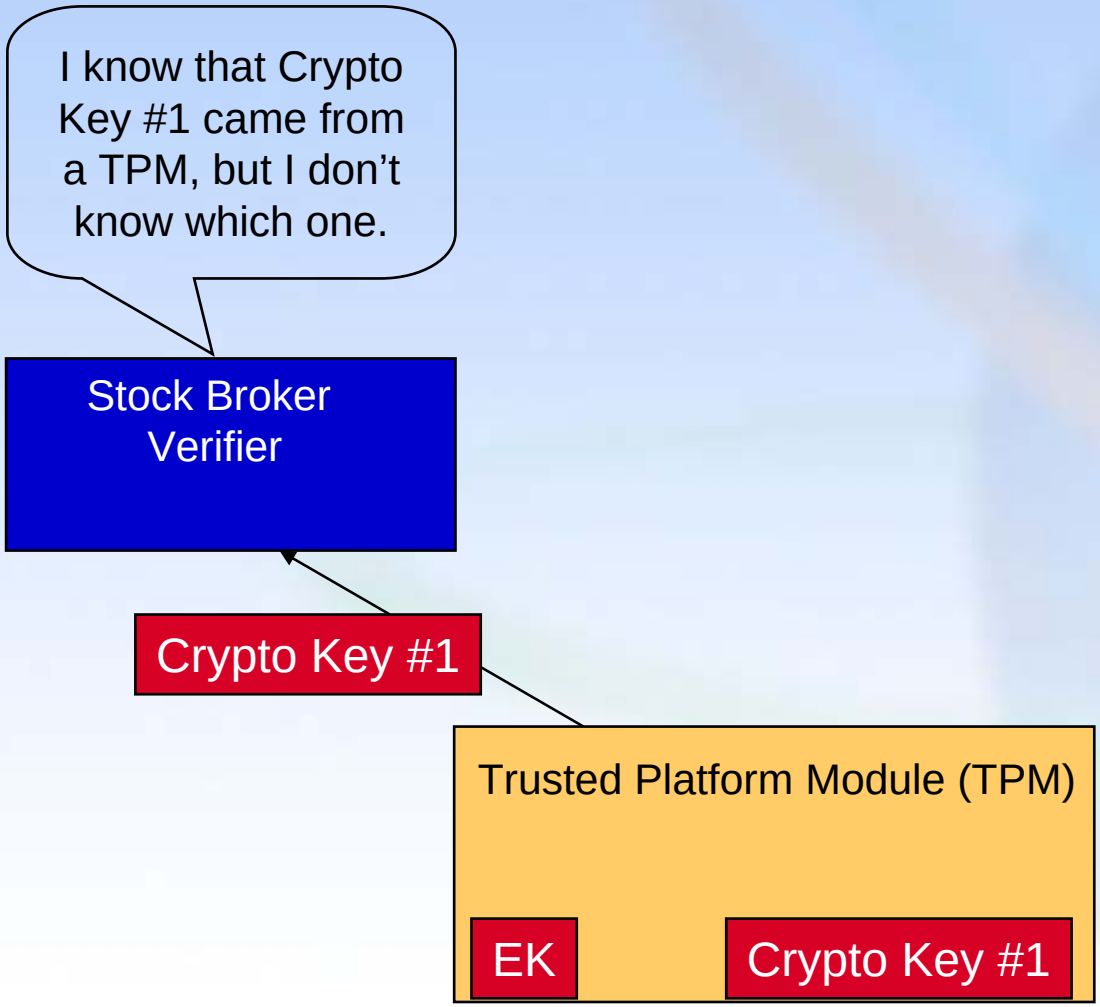
- Platform component defined by the Trusted Computing Group (TCG)
- Properties
  - Device manufactured to meet specific security requirements
  - Device performs cryptographic operations
  - Device has nonvolatile memory and can create and store cryptographic keys
  - Each device has a unique endorsement key (EK)
- EK is used to convince external parties that a key is held in a TPM

Privacy concern

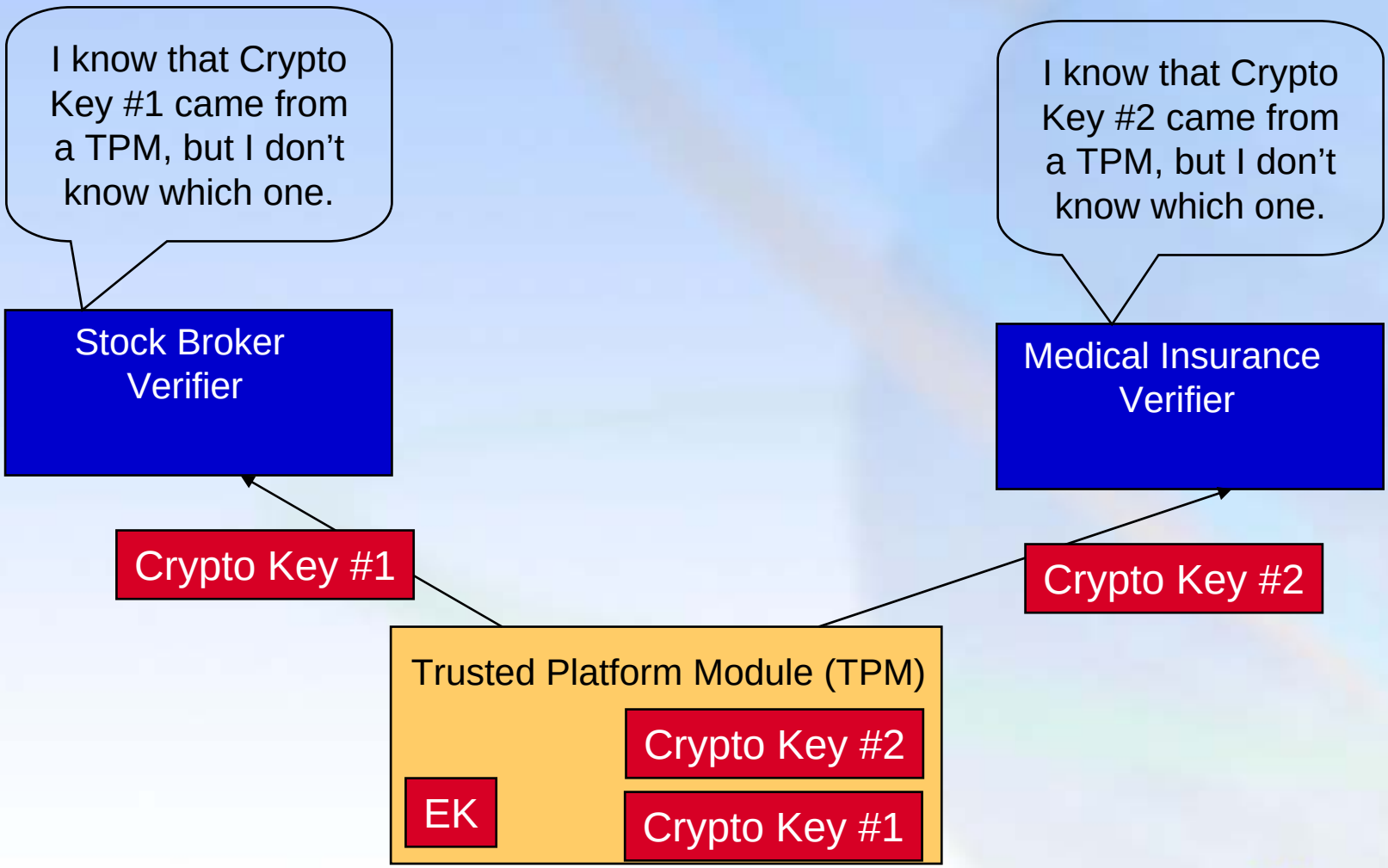
- External party may want assurance that a key is held in a TPM.
  - Example: Medical Insurance, 401K management
- The external party may not need to know the identity of the TPM
  - The unique EK should not be revealed
- We seek a solution that maximizes platform anonymity.

Problem: Convince an external party that a cryptographic key is held in a TPM without identifying the TPM.

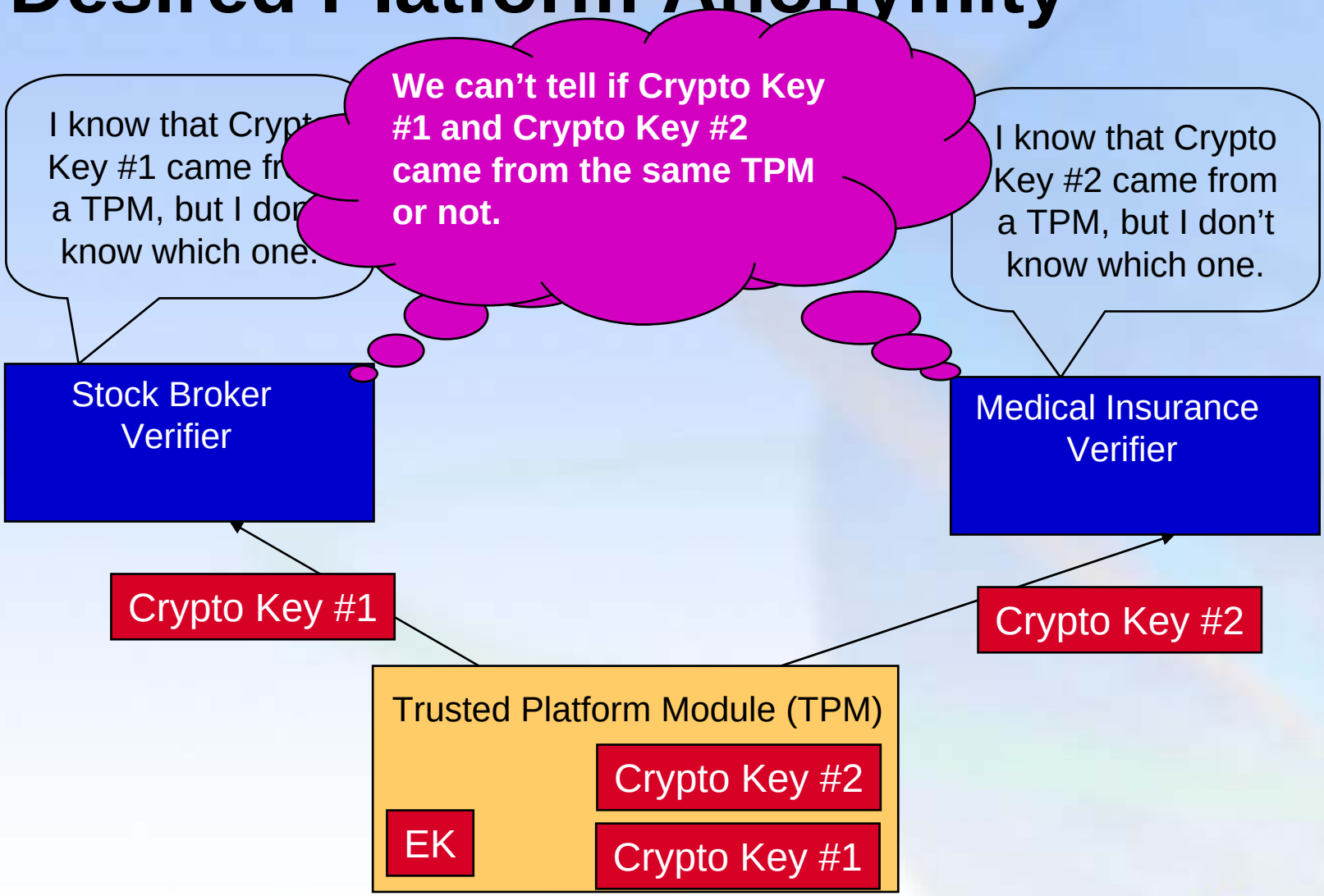
Desired Platform Anonymity



Desired Platform Anonymity



Desired Platform Anonymity



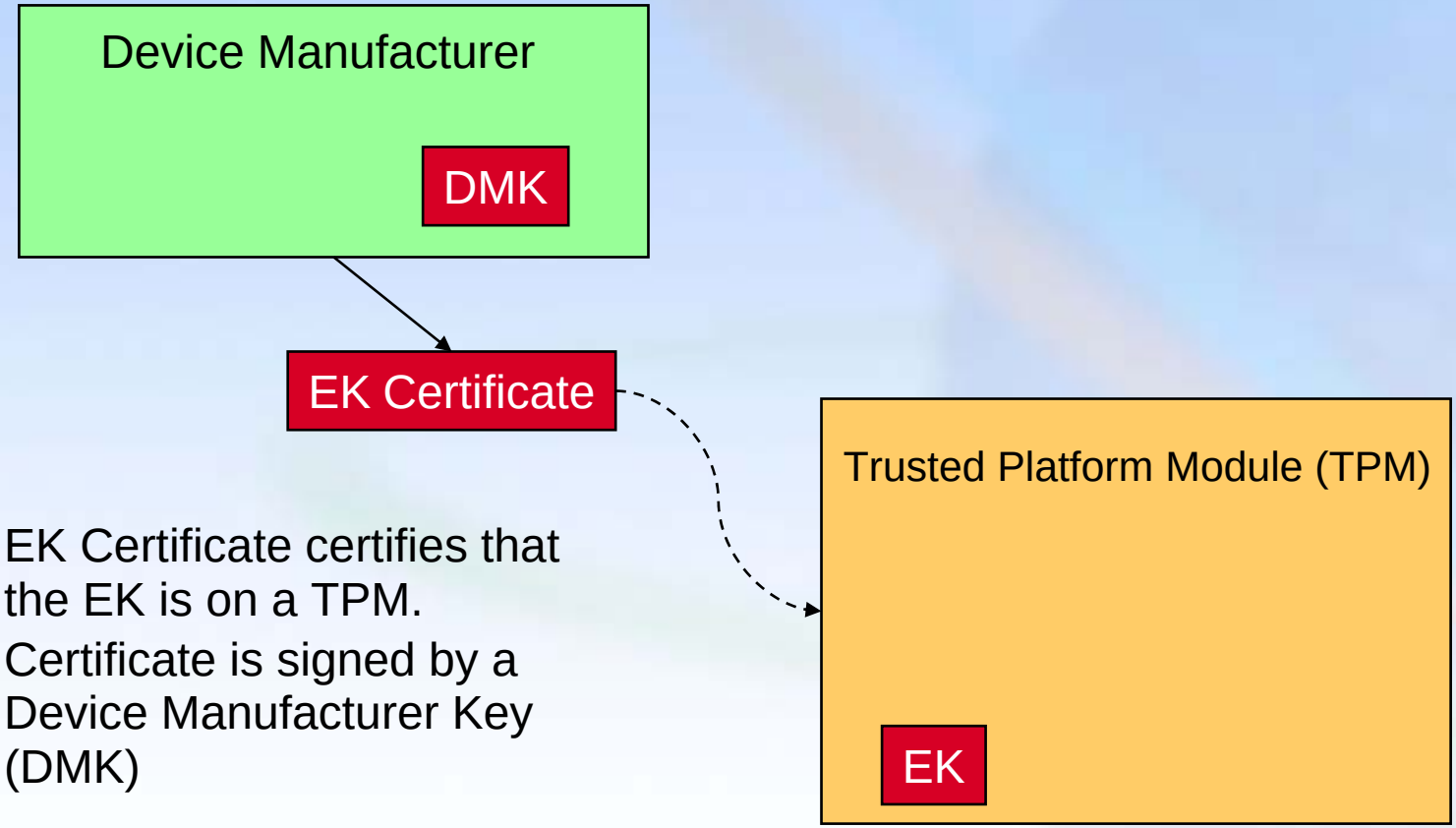
Revocation required

- An adversary with sophisticated equipment may be able to remove secret keys from an individual TPM.
- Requirements:
  - It must be possible to revoke TPM secret keys that are discovered
  - An attack on one TPM must not affect the users of any of the other TPM.

Solution options

- Certificate issued by hardware manufacturer
  - Provides no anonymity
- Certificate issued by Trusted Third Party
  - Anonymity dependent upon Trusted Third Party
- Direct Proof protocol
  - Provides anonymity without a Trusted Third Party

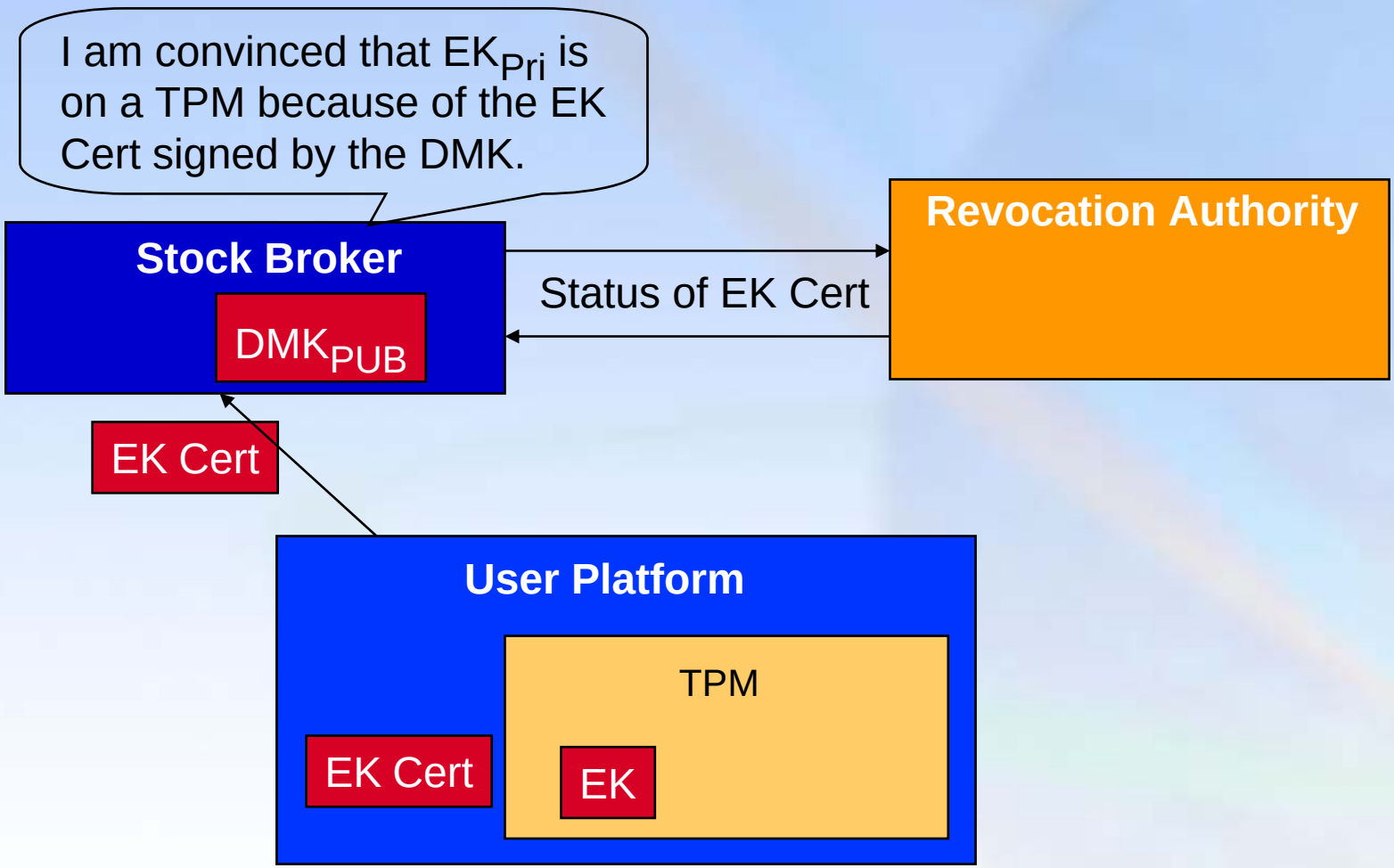
Certificate issued by hardware manufacturer



- EK Certificate certifies that the EK is on a TPM.
- Certificate is signed by a Device Manufacturer Key (DMK)

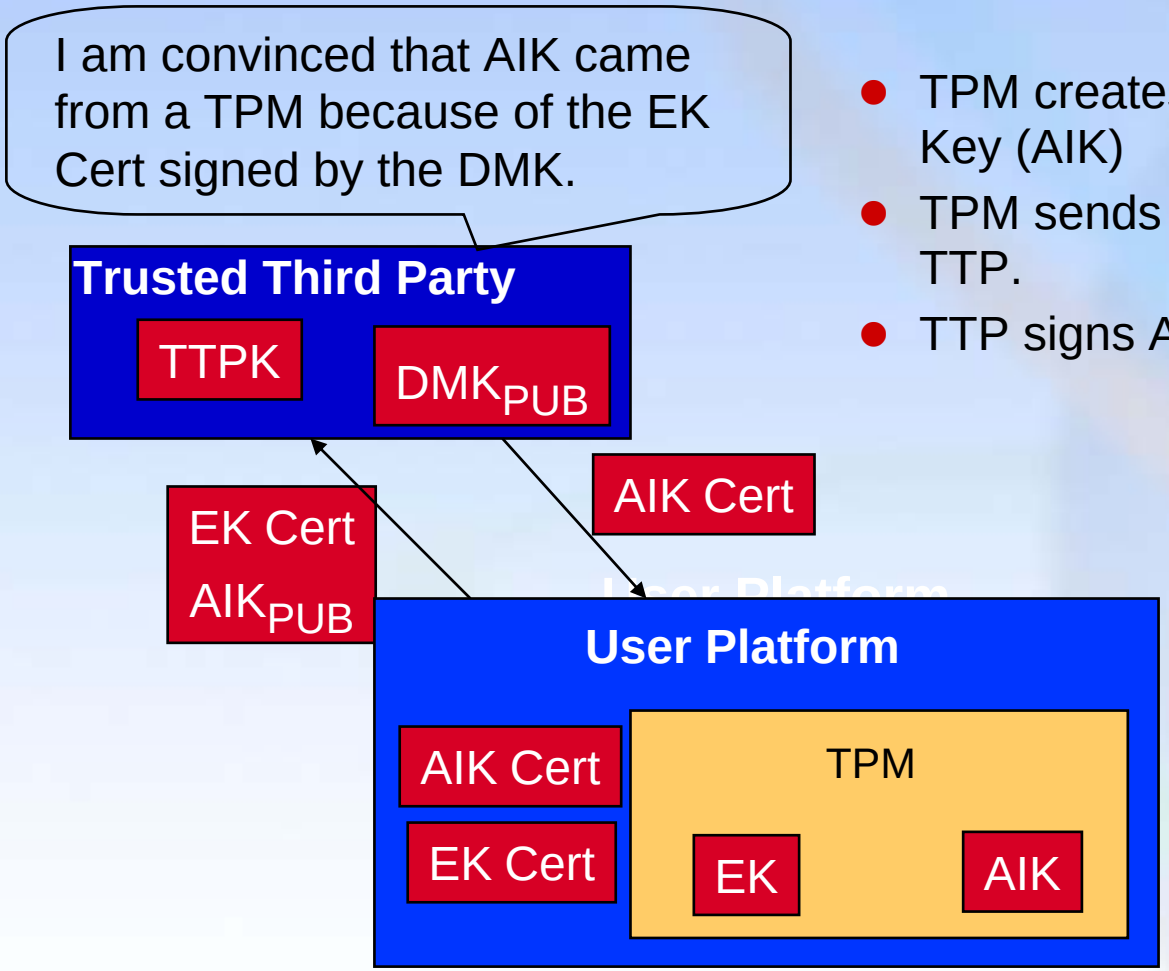
Device Manufacturer issues a unique cert for each TPM

Potential Use of EK certificate



No anonymity since EK Cert is used with every Verifier

Certificate Issued by Trusted Third Party

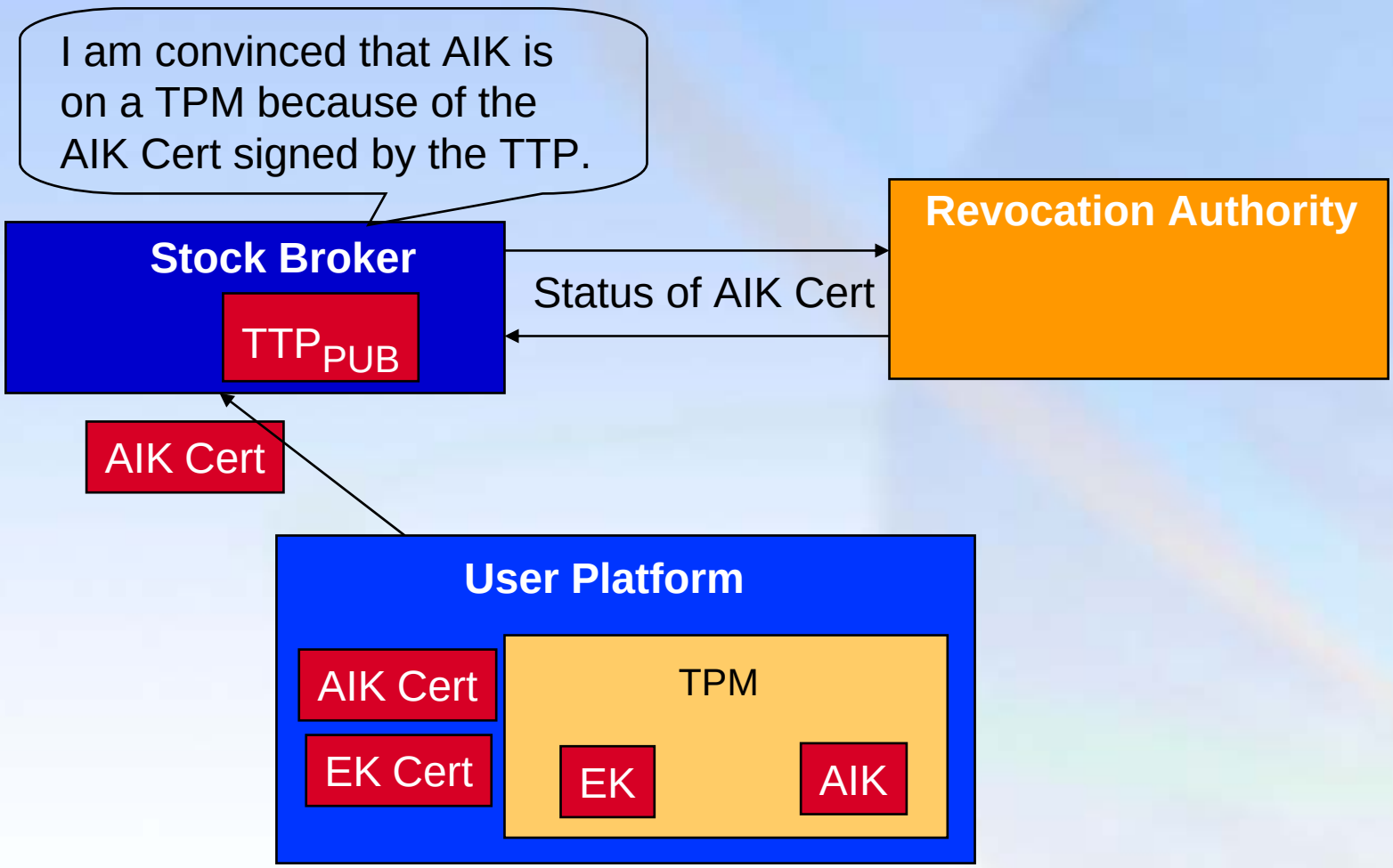


- TPM creates Attestation Identity Key (AIK)
- TPM sends AIK$_{PUB}$ and EK Cert to TTP.
- TTP signs AIK Cert with TTP Key

- AIK Cert certifies than the AIK is on a TPM

One TPM can have many AIKs

Use of TTP certificate



Anonymity is provided since different AIK Certs can be used with different Verifiers.

Requirements of Trusted Third Party

- TTP must be trusted by users and by Verifiers
  - TTP is trusted by the Verifier to NOT generate fraudulent AIK certificates.
  - TTP is trusted by the user not to reveal the relationship between the AIK and the EK
- Cost of the TTP must be paid by someone

“Zero Knowledge” Protocol - Background

- Two party protocol between
  - A prover who has some knowledge
  - A verifier who wants to be convinced that the prover has that knowledge
- Method for the prover to convince the verifier that “I know x” without revealing any information other than “the prover knows x”
- Mathematical proofs are used to show that the protocol does have the properties that are claimed

Direct Proof is a type of cryptographic protocol commonly called a zero knowledge protocol

Direct Proof– Overview

- TPM creates an AIK
- TPM uses Direct Proof to convince a Verifier that the AIK comes from a valid TPM
- TPM then uses the AIK with that Verifier exactly as it does with the TTP certificate

Direct Proof replaces the TTP certificate

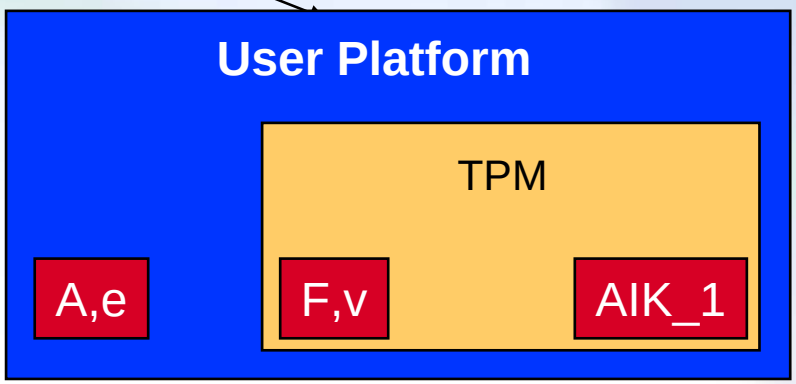
Direct Proof

I am convinced that AIK_1, $(StockBroker)^F$ mod P came from an approved TPM, but I don't know which one.

- TPM secrets: F,v
- Platform values: A,e

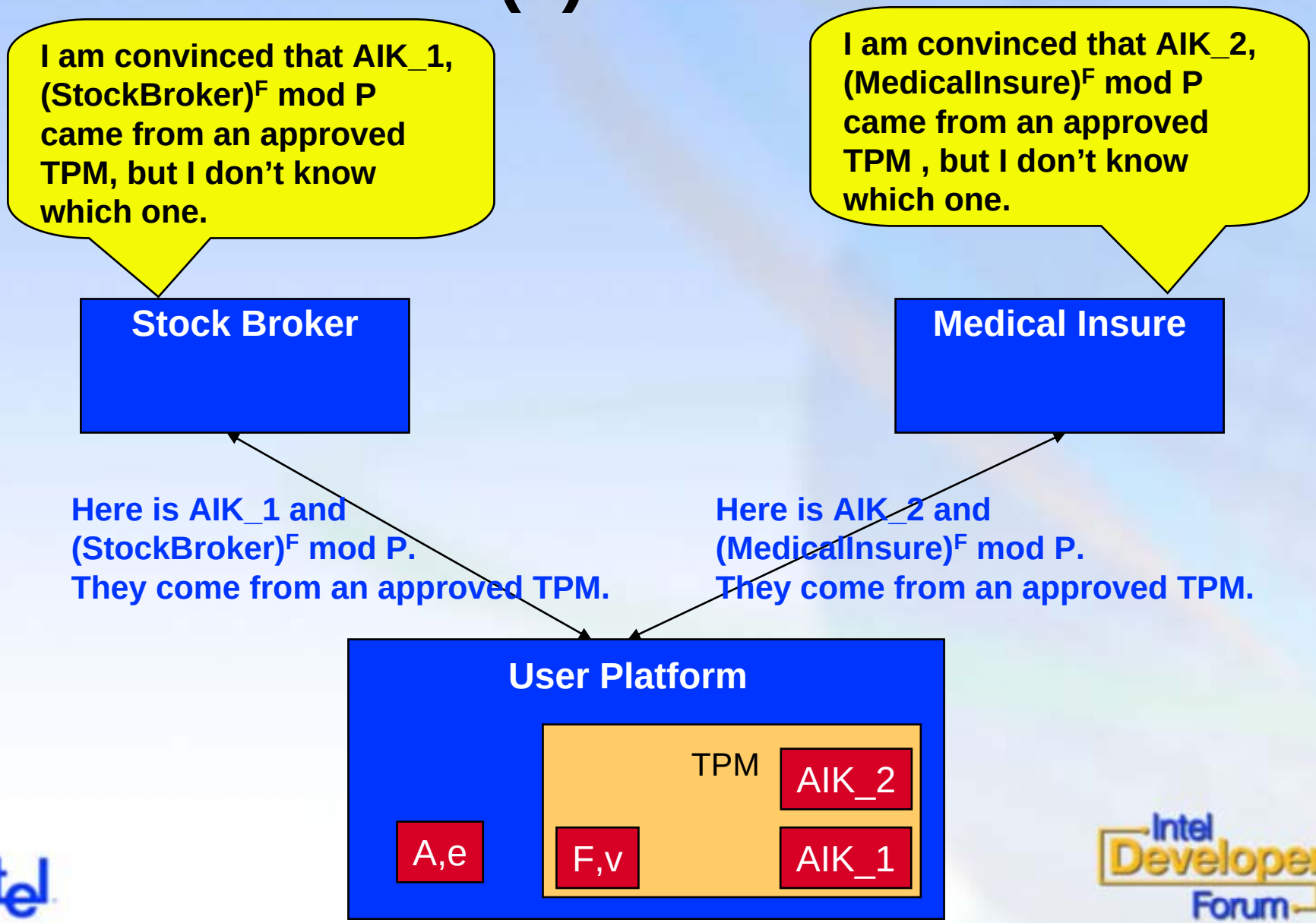
Stock Broker

Here is AIK_1 and $(StockBroker)^F$ mod P. They come from an approved TPM.

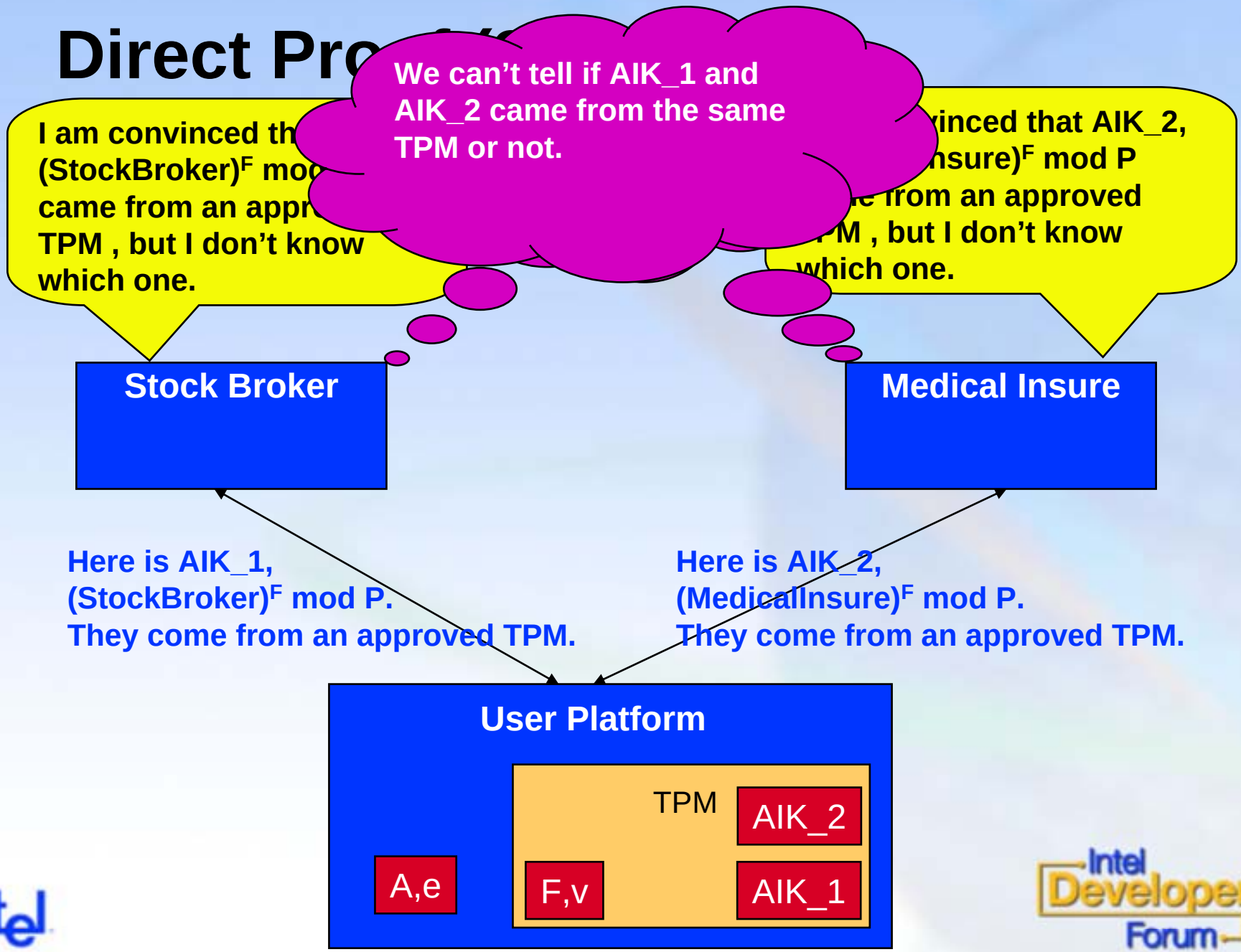


Verifier can't tell which TPM sent the AIK_1.

Direct Proof (2)



Direct Pro


We can't tell if AIK_1 and AIK_2 came from the same TPM or not.
I am convinced th
(StockBroker)F mo
came from an appr
TPM , but I don't know which one.
inced that AIK_2,
nsure)F mod P
e from an approved
PM , but I don't know which one.
Stock Broker
Medical Insure
Here is AIK_1,
(StockBroker)F mod P.
They come from an approved TPM.
Here is AIK_2,
(MedicalInsure)F mod P.
They come from an approved TPM.
User Platform
TPM
AIK_2
A,e
F,v
AIK_1

Revocation

- An adversary might take a TPM, and through a physical attack, remove the TPM secrets.
- If the adversary could give the TPM and platform secrets to others
  - TPM secrets and platform secrets are both required to perform a Direct Proof.
- If the TPM and platform secrets get published, then a verifier can
  - Check that they are valid.
  - Reject any DP that uses $(BASE)^F$ mod P
  - Note: No revocation authority needed

A Verifier can easily revoke if he has all of the keys.

Revocation (2)

- What if DP secrets get used covertly?
- If StockBroker sees many different platforms using the same DP secret,
  - i.e. the same $(\text{StockBroker})^F \bmod P$,
  - then he can start rejecting this DP secret
- This does not depend on the creation of a centralized revocation agency, which is undesirable and impractical.

Proof of Direct Proof Protocol

- We have a proof that the Direct Proof Protocol is secure given specific cryptographic assumptions:
  - Strong RSA assumption
  - Decision Diffie Hellman assumption
- Proof has been reviewed by other cryptographic experts.

TCG status on Direct Proof

- TCG is actively working on the specification
- Implementation involves only additional firmware on the TPM

Manufacturability issues

- Options for issuing Direct Proof keys to a TPM
  - At same time as issuance of the EK credential
  - At a later time, using the EK credential for trust
- Method provided for recovery from compromise of the issuer private key
- Method provided for replacing a lost DP key

Software requirements

- Client software
  - Accept requests for a Direct Proof
  - Perform the platform portions of the protocol
  - Send the necessary commands to the TPM
  - Track usage of Direct Proof and provide reports to user
  - UI for usage of Direct Proof
- Server software
  - Perform requests for a Direct Proof
  - Receive response from a Platform
  - Perform verification routines
  - Store results
- Issuer software
  - Issue DP keys
  - Store values used to replace lost DP keys
  - Protection of keys used to issue DP keys

Summary

- The Direct Proof Protocol…
  - Establishes assurance that a key came from a valid hardware security device
  - Provides platform anonymity
  - Does not require an external TTP certificate on the key

Thank you for attending.

Please fill out the Session Evaluation Form.