Implementing TCG technologies with TEE

Jon Geater,

Chief Product and Technology Officer

Trustonic Ltd

Your speaker

- I am speaking today on behalf of TCG, but of course I have other hats too which I should disclose.
- In TCG I am a member of the MPWG and the OEC. I also participate in the TPMPP certification effort.
- In GP I am on the Board of Directors and am chair of the Security Task Force.
- I also work for Trustonic, a commercial vendor of TEE software and services.
- And of course there are many other smart folks around me in all three contexts.

The beauty of standards…

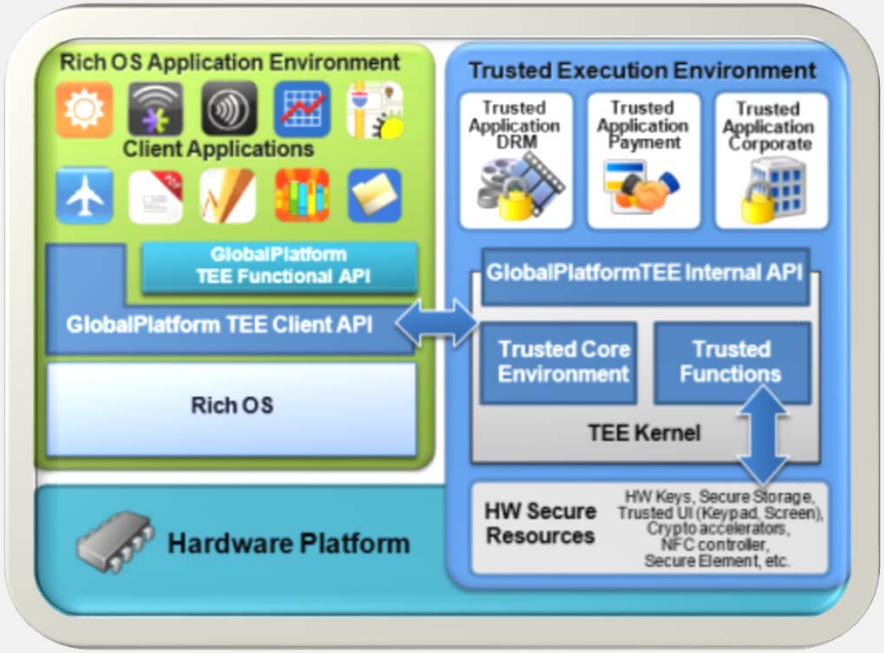
"The beauty of standards is that there are so many to choose from"

Complimentary standards

We sometimes hear people ask "TEE or TPM?" but this is not the right question…

GlobalPlatform TEE

"TEE is a separate execution environment that runs alongside the Rich OS and provides security services to that rich environment. The TEE isolates access to its hardware and software security resources from the Rich OS and its applications."



Source: GlobalPlatform TEE Whitepaper

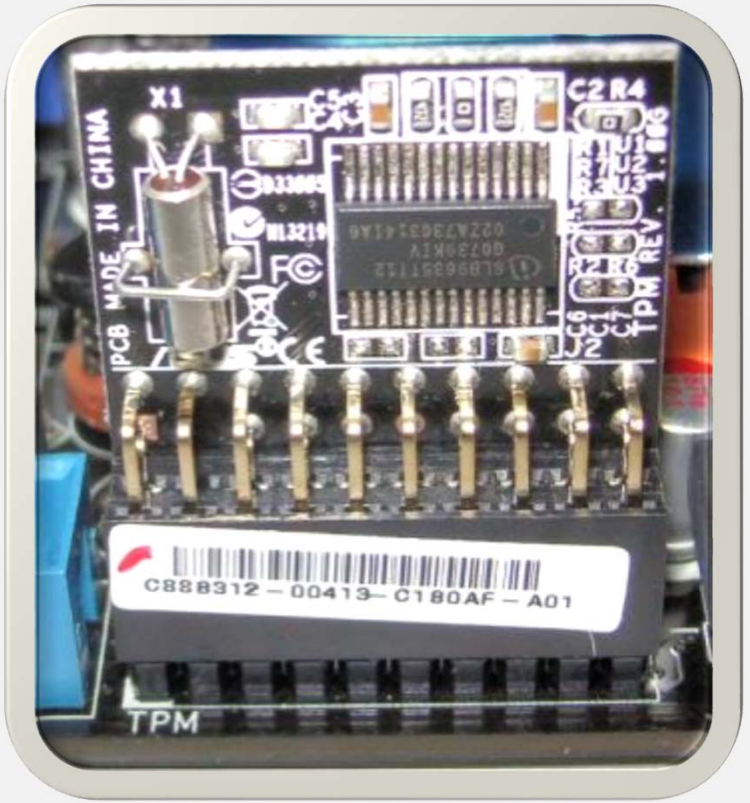
Complimentary standards

We sometimes hear people ask “TEE or TPM?” but this is not the right question…

TPM

“Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.”

“The TPM main specification is an industry specification that enables trust in computing platforms in general.”



Complimentary standards

We sometimes hear people ask "TEE or TPM?" but this is not the right question…

GlobalPlatform TEE

- Platform level
- Clients write applications inside TEE to implement custom security models
- Programmable – supports many applications and custom interfaces
- Proactive focus to secure individual applications

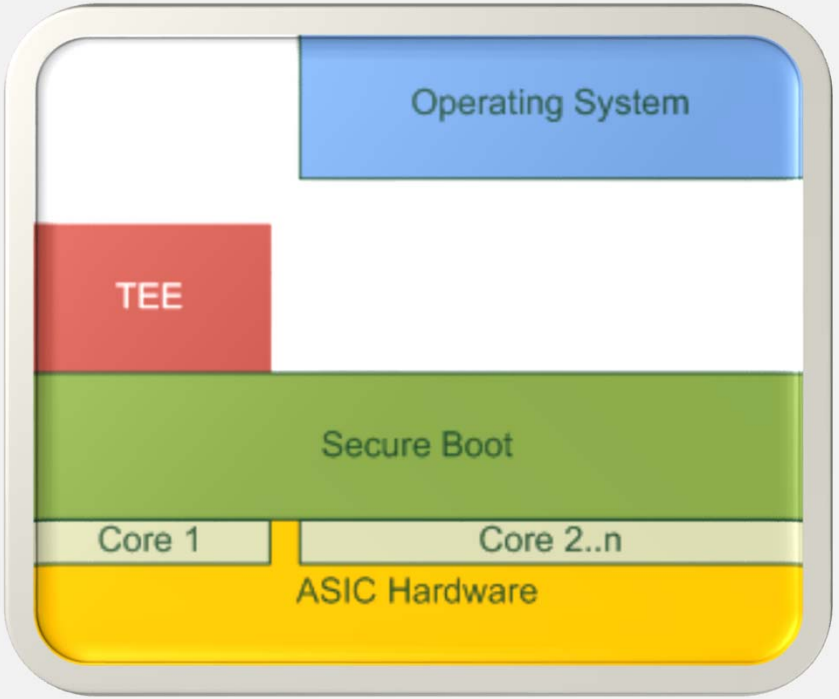
TPM Mobile

- Protocol/interface level
- Clients write applications that use the TPM security model directly
- Fixed function – uses built-in firmware to implement standard features & interface
- Defensive focus to secure broad platforms

They do different things and can be used together…

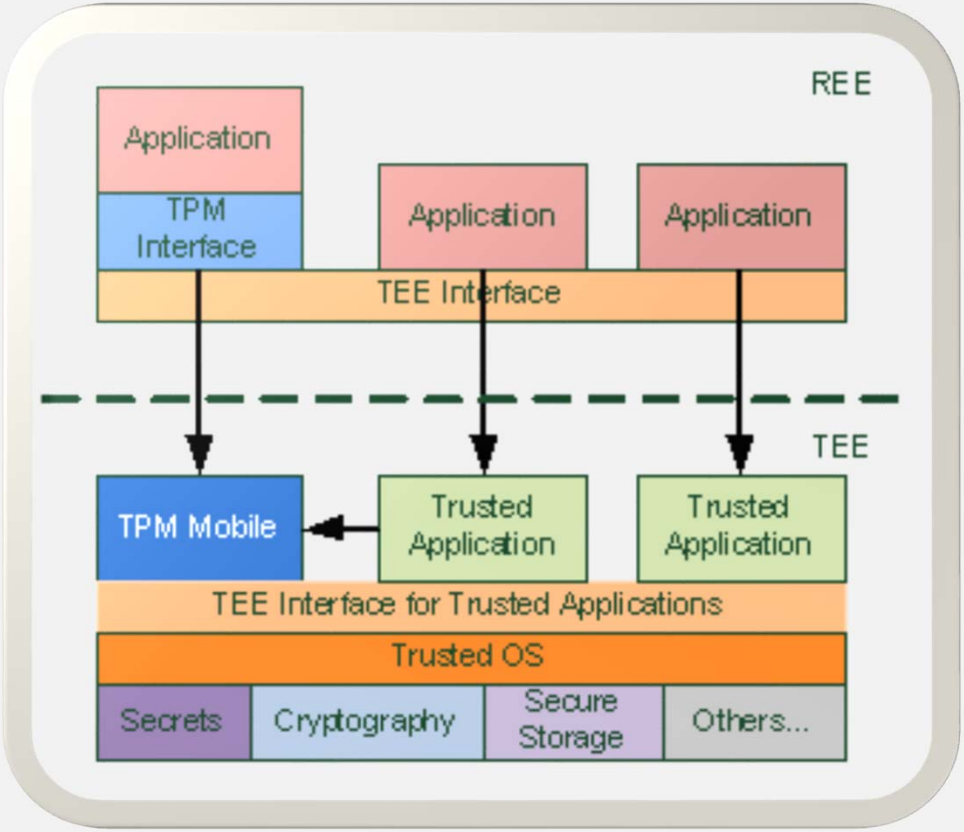
History of TPM Mobile

- **The original Mobile Trusted module (MTM) came out of TPM 1.2 but was quite different from a discrete TPM**
- **TPM Mobile is much closer to normal TPM 2.0, thanks to some good refactoring in TCG and improvements in mobile device capabilities.**
- **Both versions executed as a TA or 'firmware' and adapt to the mobile capabilities/use case.**



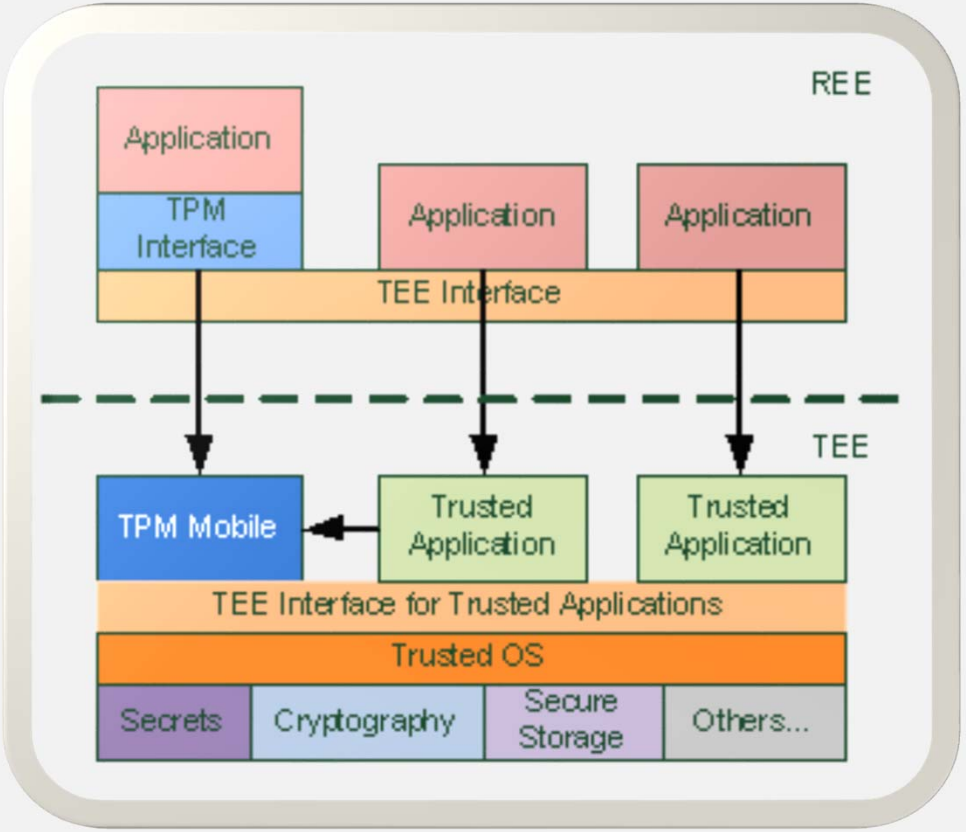
Current block architecture

- **TPM Mobile is implementable as a Trusted Application (TA) executing within a TEE which satisfies the requirements for a host environment as defined in section**
- **The roots of trust of the TPM Mobile must be supported by the TEE architecture and implementation.**



Current block architecture

- **TEE provides platform integrity, isolated execution and access to hardware-based roots of trust**
- **By implementing as a TA you also retain all the capabilities of the TEE for other applications which do not use TPM**



Better Together (i)

TPM provides excellent primitives for device integrity and key storage features, but if you try to bend it to other use cases it can become unwieldy, becoming complex and having atomicity issues, etc. Compare this code to a simple smartcard signing use-case:

$d'_0 \leftarrow$ TPM2_StartAuthSession(
    <$objectHandle_{ctr}$, $sessionType_{policy}$>, <$sessionhandle_{ctr}$>)
$d'_1 \leftarrow$ TPM2_PolicyCommandCode(<TPM_CC_NV_READ>)
    TPM2_NV_Read(<$sessionhandle_{ctr}$, ctr>, <n>)

$d_3 \leftarrow$ TPM2_PolicyNV(<$sessionHandle_{eID}$, ctr, n, eq>)

$d''_0 \leftarrow$ TPM2_StartAuthSession(
    <$keyHandle_{ctr'}$, $sessionType_{policy}$>, <$sessionHandle_{ctr'}$>)
$d''_1 \leftarrow$ TPM2_PolicyCommandCode(<TPM_CC_NV_Increment>)
    TPM2_NV_Increment(<$sessionhandle_{ctr}$, ctr>)

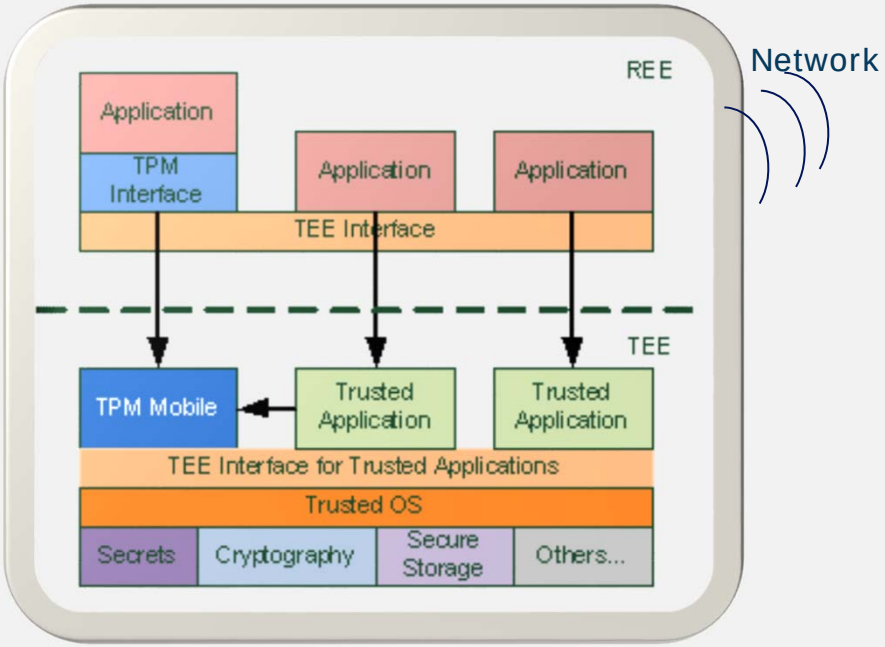
$d_{(n,n+1)} \leftarrow$ TPM2_PolicyNV($sessionHandle_{eID}$, <ctr, $n+1$, eq>)
$d_4 \leftarrow$ TPM2_PolicyOR(<$sessionHandle_{eID}$, $d_{(0,1)}$, $d_{(1,2)}$, $d_{(2,3)}$>)
    [counter reset]
    TPM2_VerifySignature(<$keyHandle_A$, $signature_b$>, <$ticket_{\{b,A\}}$>)
$d_5 \leftarrow$ TPM2_PolicyAuthorize(
    <$sessionHandle_{eID}$, $signature_b$, $policyRef_b$,
    $keyName_A$, $ticket_{\{b,A\}}$>)

Better Together (i)

But equally well if you have a TPM platform use case that is well supported by the specification it may be unappealing to write a whole Trusted Application for the TEE

Source: http://commons.wikimedia.org/wiki/File:Typing_computer_screen_reflection.jpg
Picture by WikiMedia Commons user Almonroth

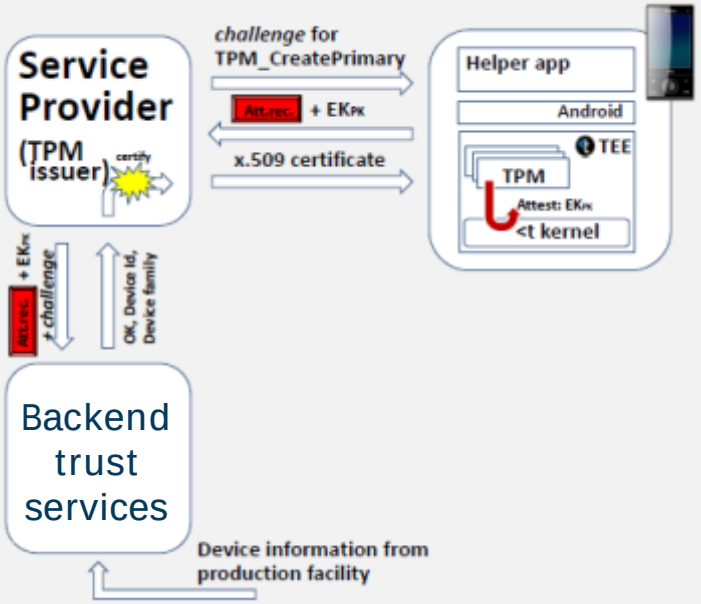
Better Together (ii)



Having both options available in the device, conscientiously integrated, gives the best options to device makers/users and should increase the popularity of both technologies.

Better Together (ii)

- **Implementing the TPM in TEE enables some old difficulties with platform key management, refurbishment etc.**
- **EK hierarches can be refreshed, or even provisioned after market thanks to roots of trust and attestation features in the TEE**
- **More choice for participants in the highly dynamic world of mobile devices.**



Demonstrator

- **This is real!**
- **TCG held a successful one-day seminar at the RSA Conference this year called "Get Proactive With Security"**
- **We showed a demonstrator with a partial TPM implementation running in a TEE on a commercially available off-the-shelf tablet device.**
- **Whitepaper available from Trustonic**

TCG materials

- **Main TPM library spec (2014)**
  http://www.trustedcomputinggroup.org/resources/tpm_library_specification
- **Mobile use cases (2011)**
  http://www.trustedcomputinggroup.org/resources/mobile_trusted_module_20_use_cases
- **Mobile reference architecture (2014)**
  http://www.trustedcomputinggroup.org/resources/tpm_20_mobile_reference_architecture_specification
- **Mobile whitepaper (2012)**
  http://www.trustedcomputinggroup.org/resources/tpm_mobile_with_trusted_execution_environment_for_comprehensive_mobile_device_security

Questions?

?