Trusted Execution Environments (and Android)

Jan-Erik Ekberg
Director of Advanced Development, Trustonic
9.9.2015

TRUSTONIC

Content:

1) What is a TEE

2) TEE on Android (today)

3) (Research) use cases

TRUSTONIC

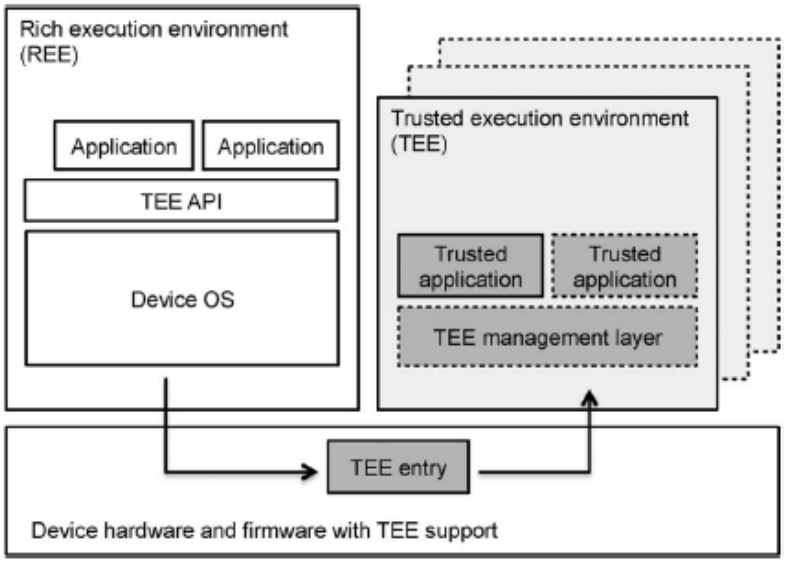
What is a TEE (Trusted Execution Environment)

Hardware-assisted isolated execution
- from ”normal world OS” and
- between ”trusted applications”

Integrity of operation
- ”part of” secure boot
- trusted path
- rollback protection

(Unique) access to secrets
- secure storage
- device authentication
- remote attestation

(Availability)
- code provisioning

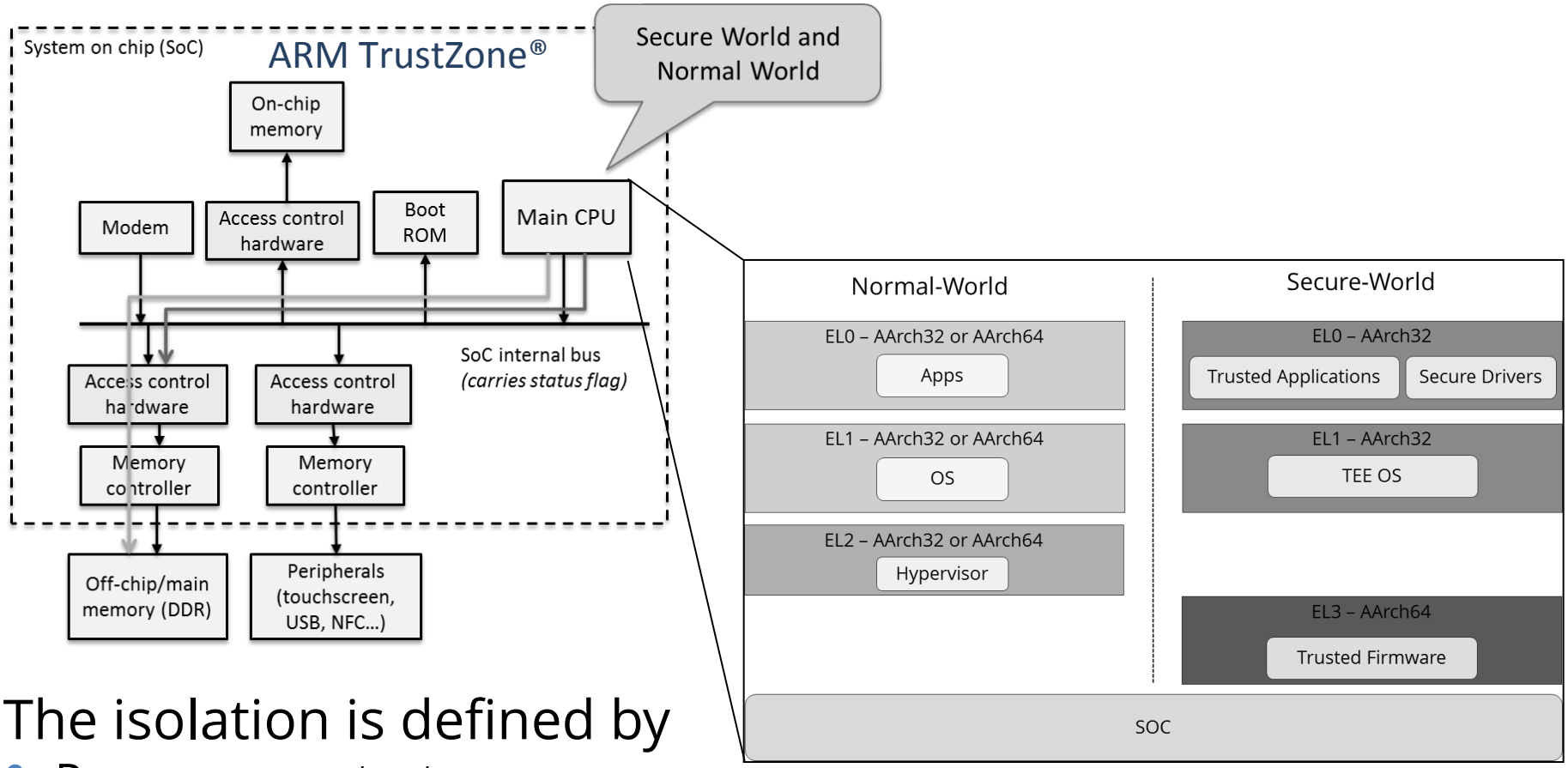


Typical properties
- fast / full memory access
- runs at full processor speed
- ”native binaries / ”standard C”

Ref & reading: [1] Vasudevan & al., [2] Asokan & al, [3] Ekberg & al

TRUSTONIC

TEE HW in 2015? ARM Trustzone?



The isolation is defined by

- Processor contexts
- Memory access / MMU, caches
- DMA / IRQs

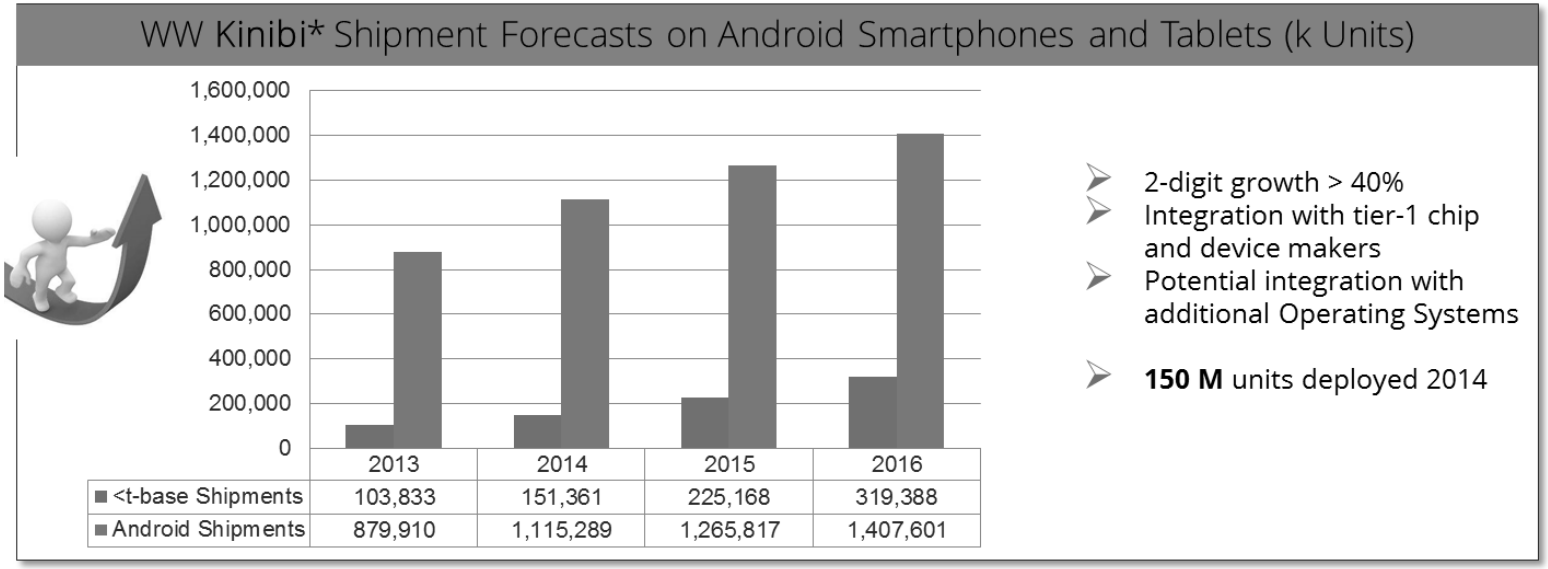
New HW architectures are emerging:

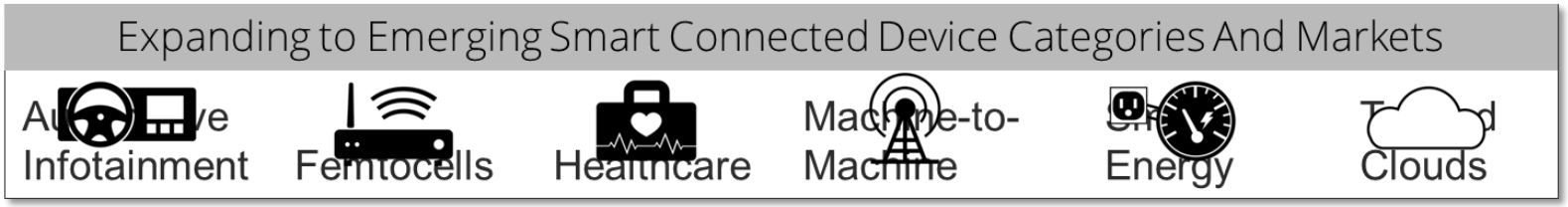
- Intel SGX / TrustLite (research)

TRUSTONIC

Where do we find TEEs today?

- Most(many) middle to high-end Android & Windows phones
- Set-top boxes, tablets & laptops

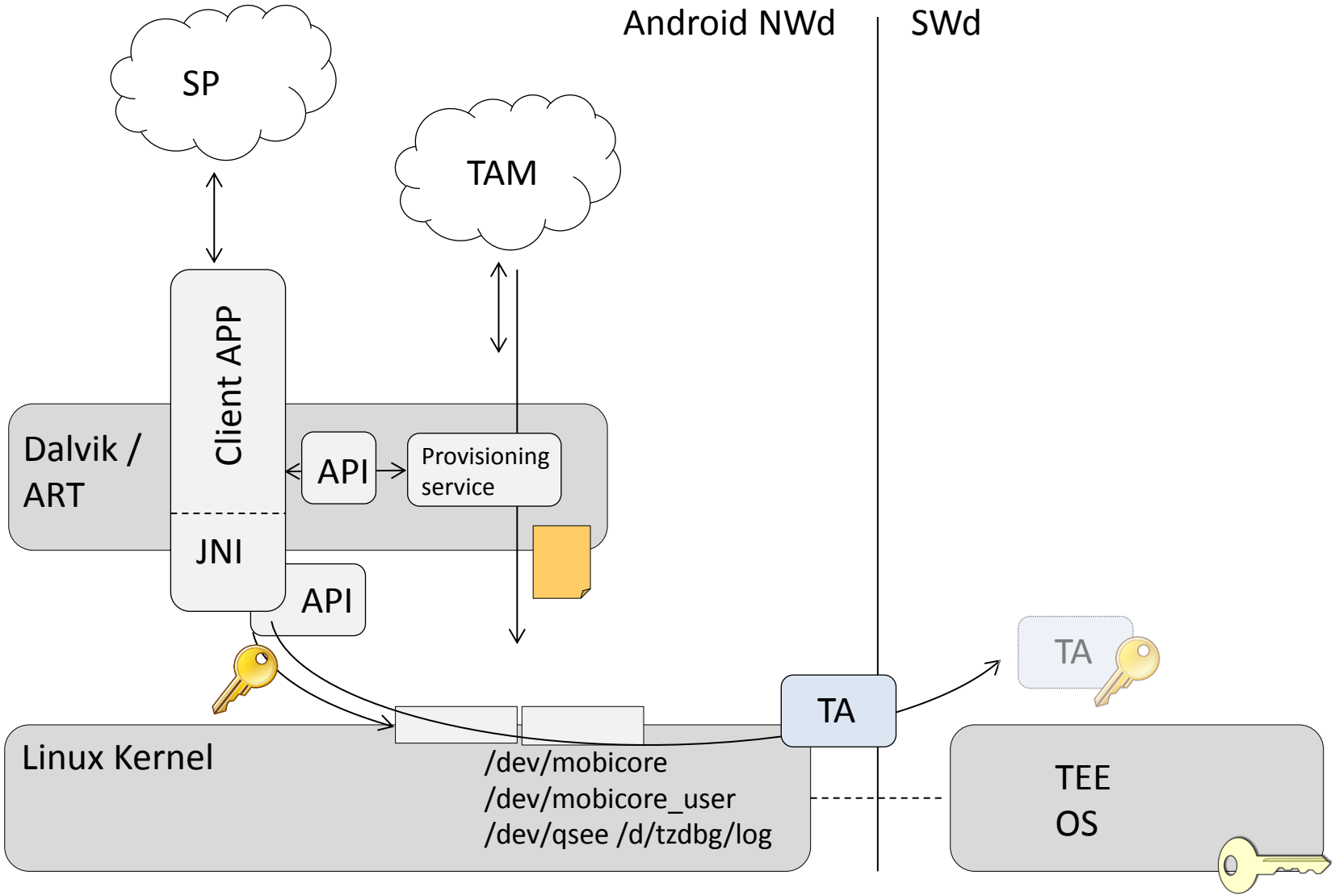




*Gartner 2013, Trustonic Market Intelligence
*Take into account high-end devices only – Trustonic already has mid-end devices in scope
*Trustonic partnerships with Major MNOs will largely boost these figures

TRUSTONIC

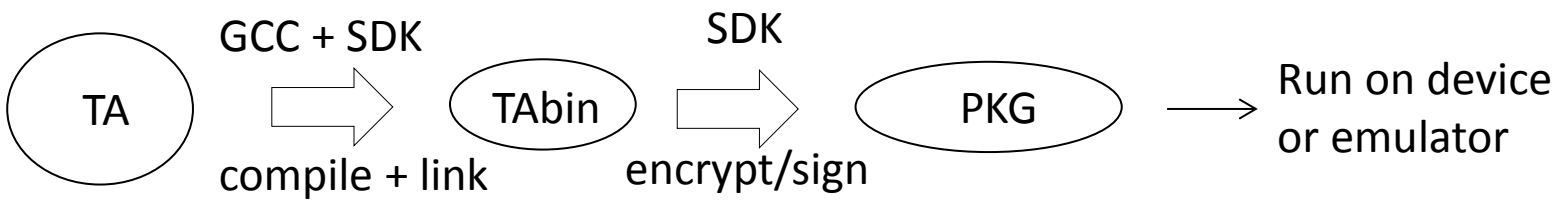
TEE usage on Android (Android 4.1→~5)



Simple Trusted Application

A legacy TA. (A TA using standard GP TEE API does not fit on a slide)

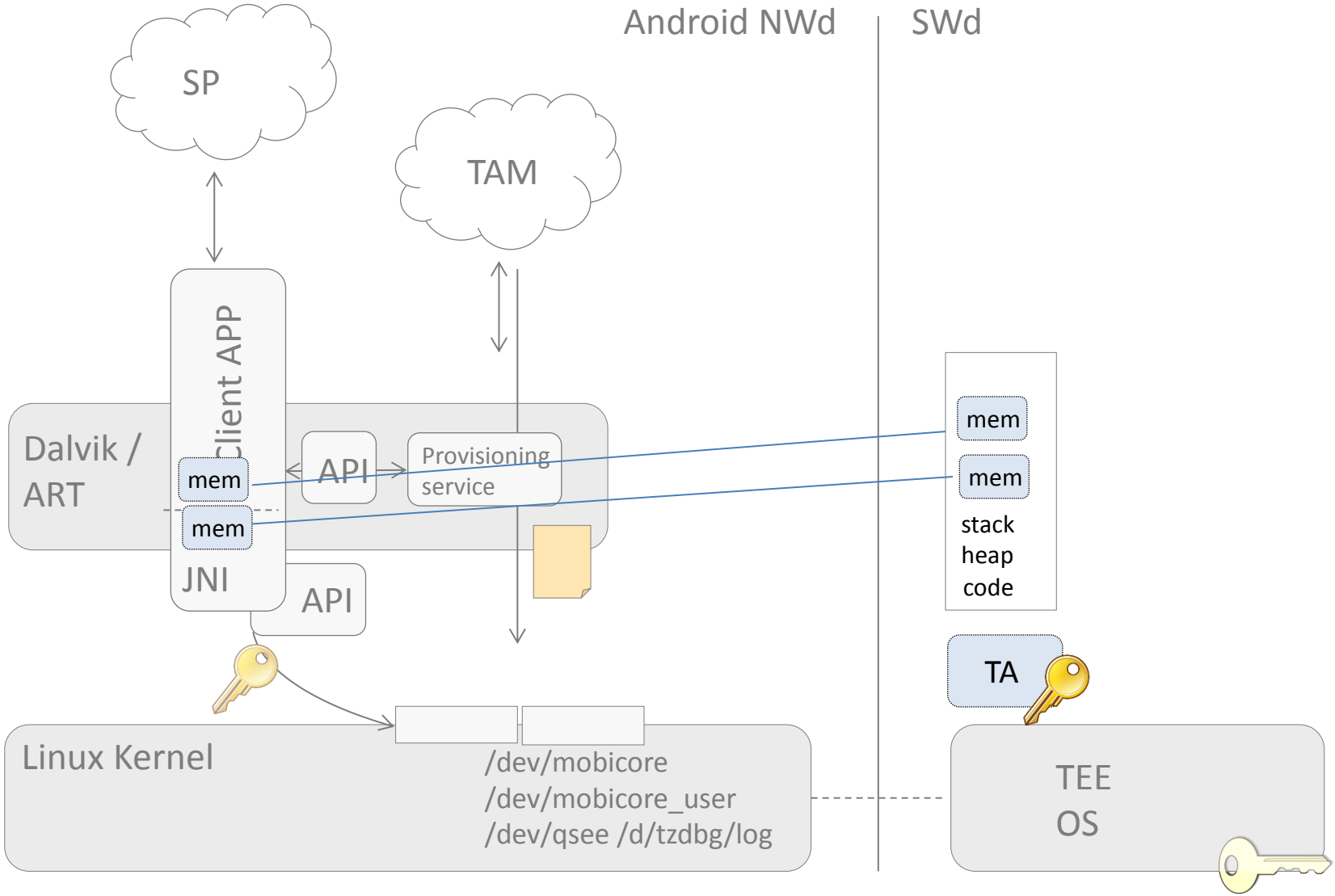
```
_TLAPI_ENTRY void tlMain(const addr_t buf,const uint32_t len)
{
     uint32_t secbuf;
     if ((NULL==buf)||(buflen!=4)||!tlApiIsNwdBufferValid(buf, 4))
        tlApiExit(EXIT_ERROR);

    for (;;)
    {
      tlApiWaitNotification(TLAPI_INFINITE_TIMEOUT);
      memcpy(&secbuf,buf,4); secbuf |= 0xDEAD; memcpy(buf,&secbuf,4);
      tlApiNotify();
    }
}
```



Open-source environments for testing GlobalPlatform TAs:
OpenTEE (D) and **OpTEE** (E)

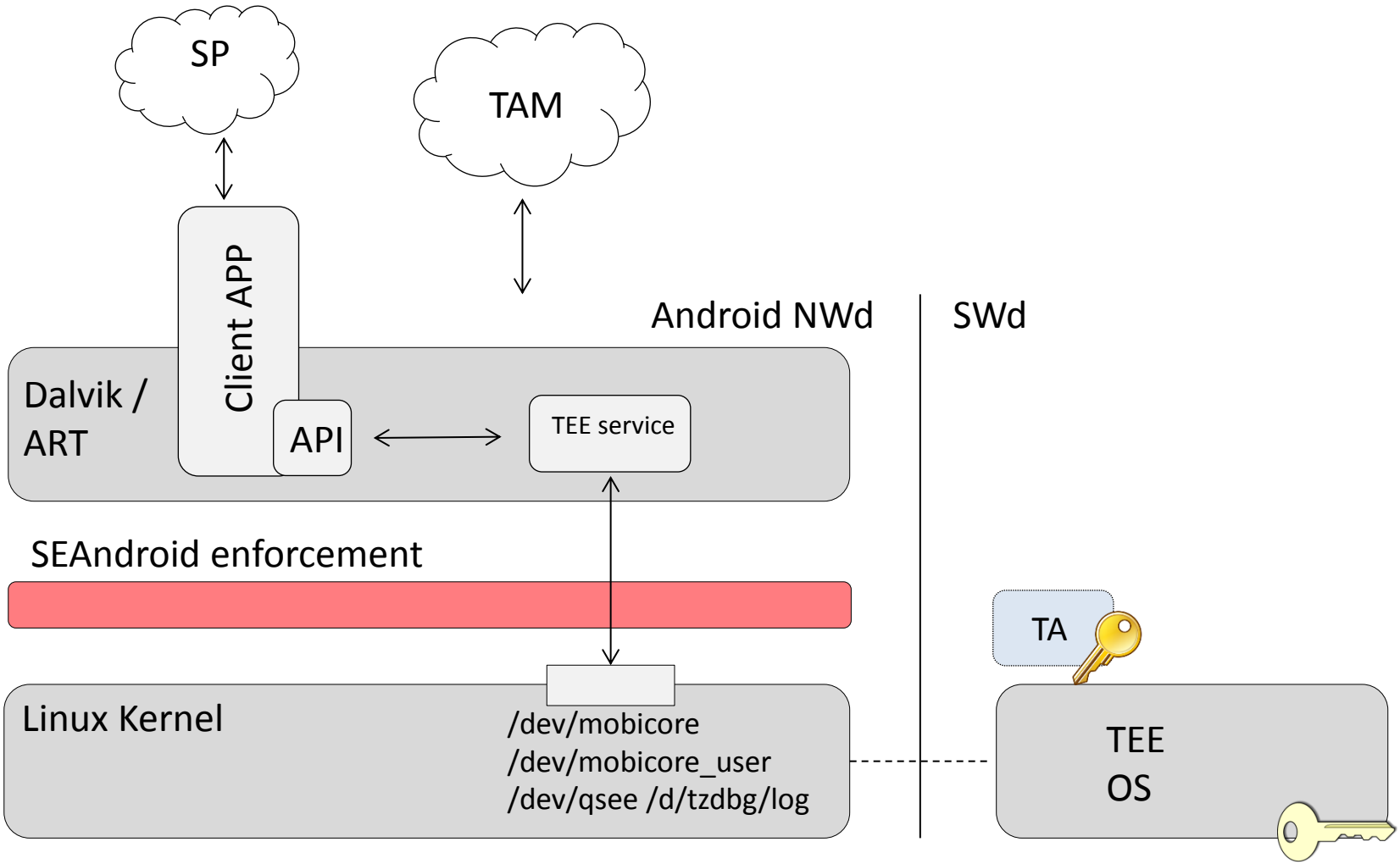
TRUSTONIC

TEE interaction (Kinibi) (Android 4.1→~4.4)



SEAndroid will change things to come in Android6 →

- A problem specific to 3rd party use
- Provides for caller authentication
- Raises the abstraction level for the APIs (C→Java)



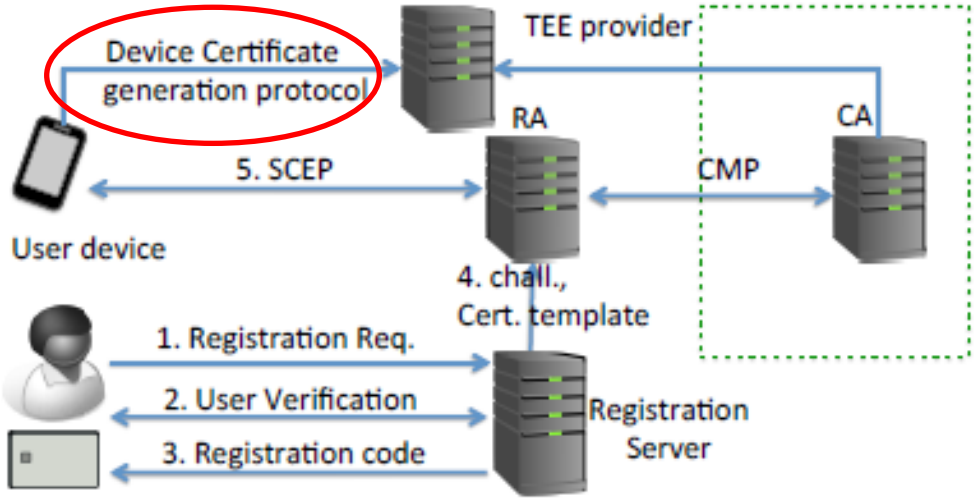
Use cases

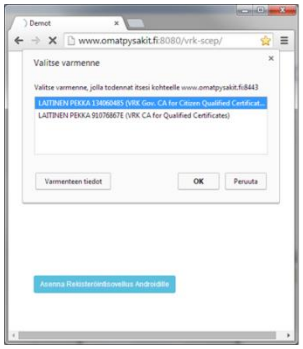
1. Citizen EId:s with TEEs

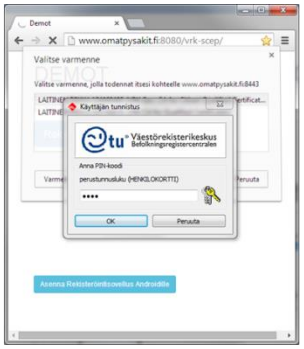
1) For TEEs, we need device **endorsment**

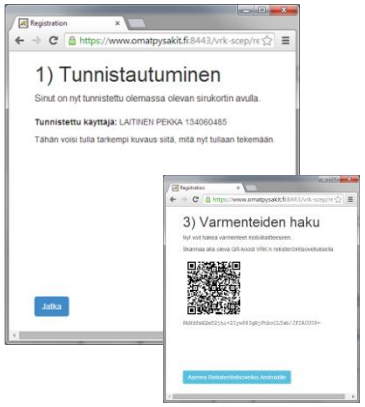
2) Enrolment different from smart cards

3) Inter-service communication not as well developed as in PC context







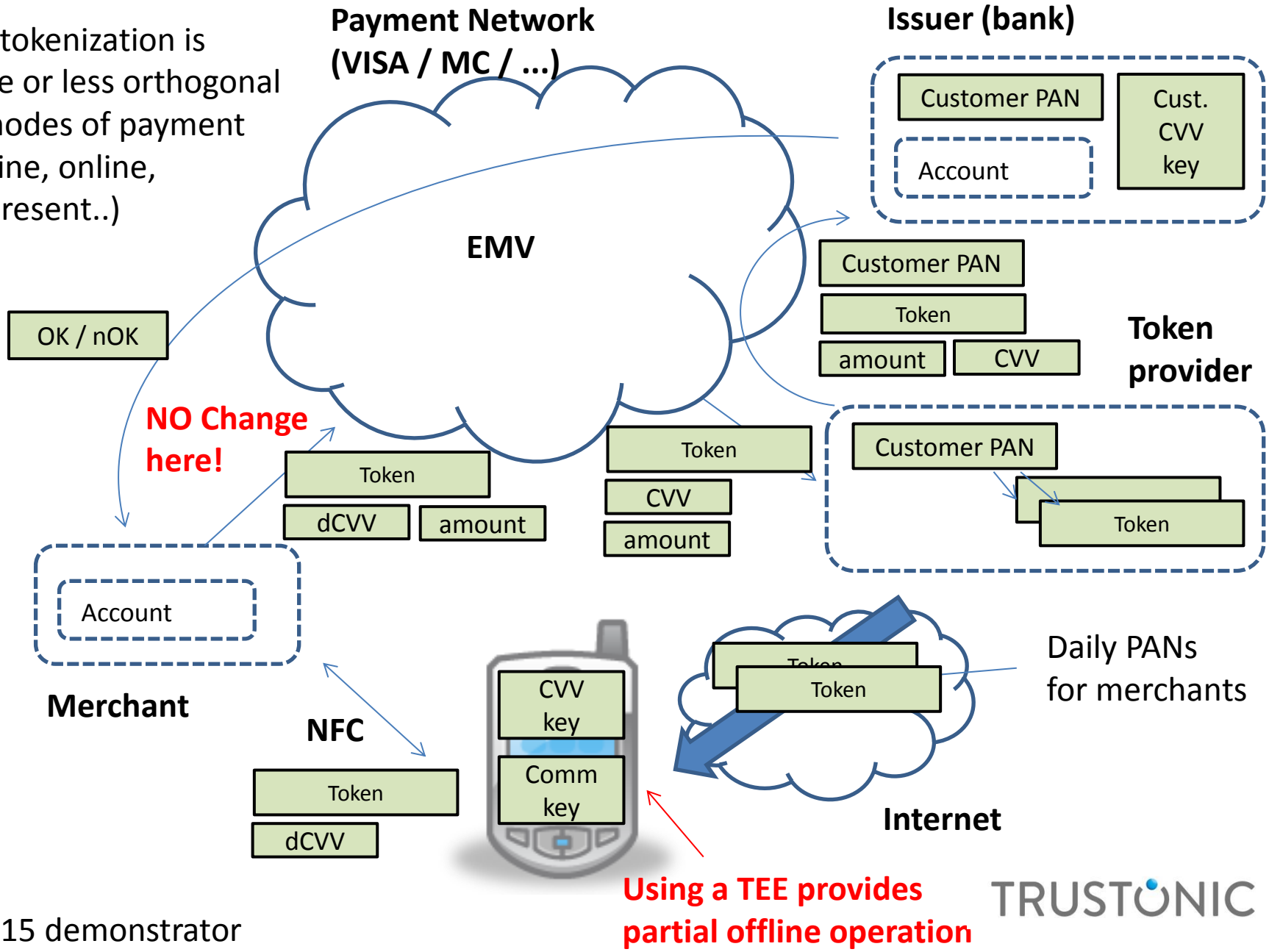


Tamrakar & al: [F]

TRUSTONIC

2. Better EMVCo tokenization security with TEEs

The tokenization is more or less orthogonal to modes of payment (offline, online, PinPresent..)

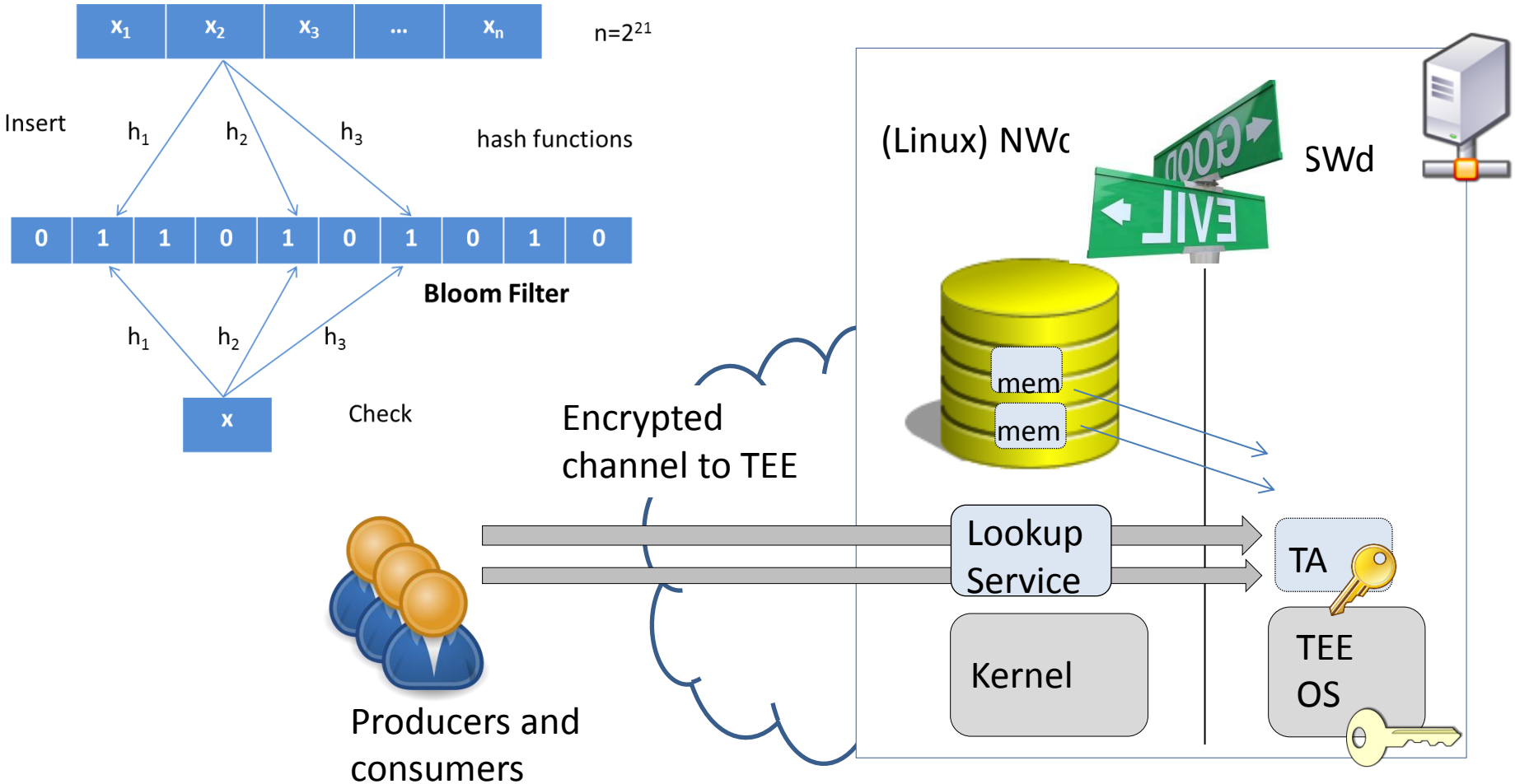


TRUSTONIC

MWC'15 demonstrator

3.Private membership lookup (in cloud)

(alternative to homomorphic enc. Solutions)



Having direct memory access separates a TEE from a smart card or HSM. Other examples include DRM and trusted path.

TRUSTONIC

Links and references

A. Vasudevan, E. Owusu, Z. Zhou, J. Newsome, and J.M. McCune. Trustworthy Execution on Mobile Devices: What security properties can my mobile platform give me? In Trust and Trustworthy Computing, vol. 7344 of LNCS, pp 159–178. Springer, 2012.

B. Asokan, N., Ekberg, J. E., Kostiainen, K., Rajan, A., Rozas, C., Sadeghi, A. R., ... & Wachsmann, C. (2014). Mobile Trusted Computing. *Proceedings of the IEEE*, *102*(8), 1189-1206.

C. Ekberg, J. E., Kostiainen, K., & Asokan, N. (2014). The untapped potential of trusted execution environments on mobile devices. *IEEE Security & Privacy*, (4), 29-37.

D. McGillion & al (2015): Open-TEE - An Open Virtual Trusted Execution Environment, TrustCom'15 (http://arxiv.org/abs/1506.07367)

E. Linaro project: https://github.com/OP-TEE/optee_os

F. Tamrakar & al (2015): On ReHoming the Eld to TEEs : IEEE TrustCom

TRUSTONIC

Thank you!
Questions?

People pay for better experiences

….security enables them

TRUSTONIC