The Device Identity Challenges

Shahrokh Shahidzadeh

March 7 2011

Intel Corp.

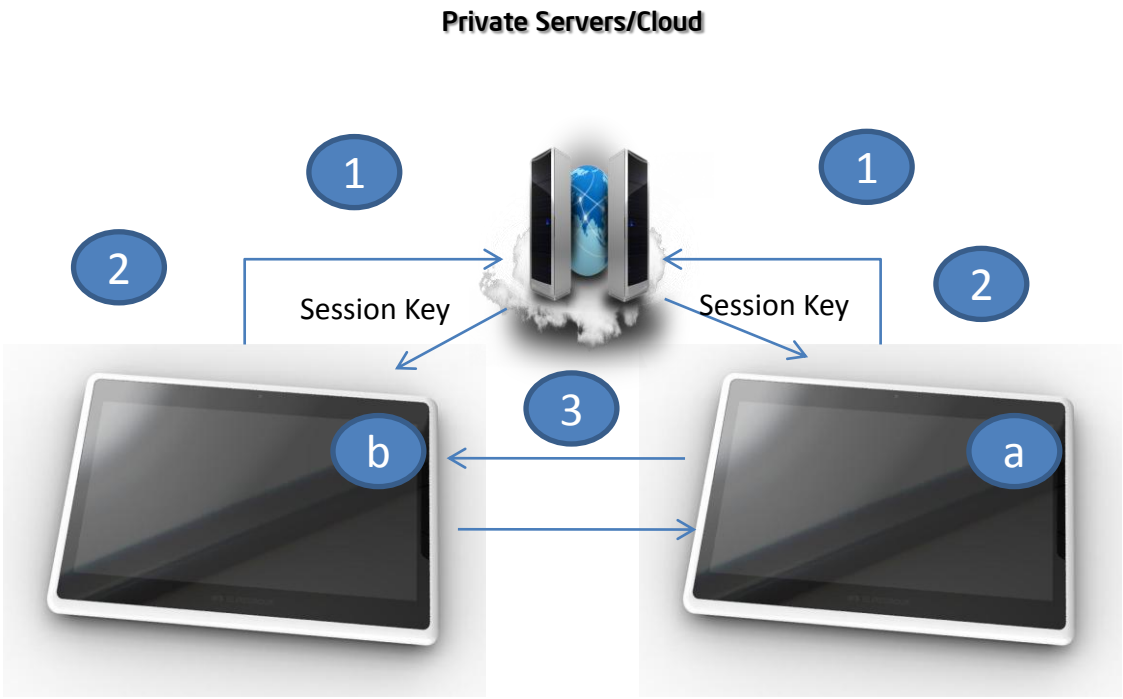
Simplistic View Of The Device Identity

- Multi Factor Authentication To Get Your Device To The Cloud Securely
- Need For Session Keys and runtime HW-SW Tokens To Generate Isolated P2P Connection

1. User ID And Password To Connect To Private Cloud

2. Device Identity Verified By The Cloud And Access Granted

3. Device Requests P2P Connection To another Banded Platform and A Session Token Is Injected → P2P Secure Session



Key Ingredients

- Need for a HW token vault and platform identity that is immutable, indisputable and tamper proof
  - Device Identity is a major building block of multi factor authenticaion)
- Need for an integrated and isolated source of Entropy
  - HW RNG
- Need some type Of HW assisted biometric
    - Identity cards make sense but expensive
- And then of course a mechanism for creating an isolated execution environment
  - Need HW Client-Aware Cloud APIs to verify identity of the End-Point Device

Need For A Dedicated Vault As Atomically Close To The Processor As Possible To Store Critical Secrets & Token Chains

- Must Be Provisionable Through Different Lifestages Of The Product
- Must Be Immutable (Portion of memory on some sort of block boundaries)
- Must Be Secured (needs a secure engine to manage it)
- Must be scalable for all formfactors (including Cell Phone)

Platform Embedded Token

Where does it need to happen?

- embedded in the hardware isolated from the OS
- The one time code is validated by a third party security ISV used by the websites

And Then The Biometric Solution We Are Looking At