Self-Encrypting Drives (SEDs) for Consumers

Robert Thibadeau, Ph.D.

Chairman & CEO

Bright Plaza, Inc.

Agenda

- Self-Encrypting Drive Technology (*What are SEDs actually?)*
- Consumer uses (*may surprise you*)
- Consumer endpoint uses (main discussion)

- Takeaways: Consumer uses *can and do work* :
- *Two Principles* are, ultimately, important (for great consumer product)

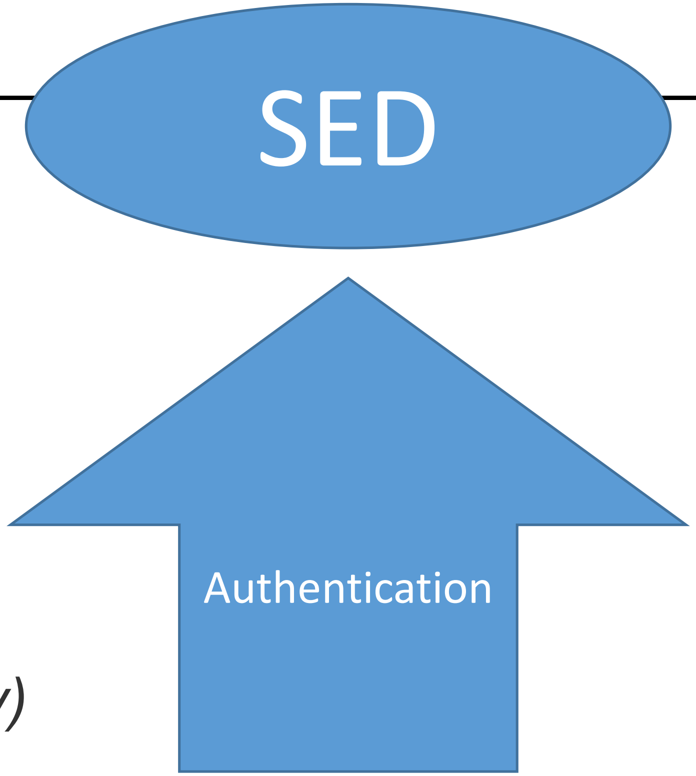
bright plaza

www.brightplaza.com

DRIVE TRUST ALLIANCE

KAJE Authentication

pronounced “cagey” (definition: crafty, shrewd, tricky)



Bright Plaza, Inc and the Drive Trust Alliance

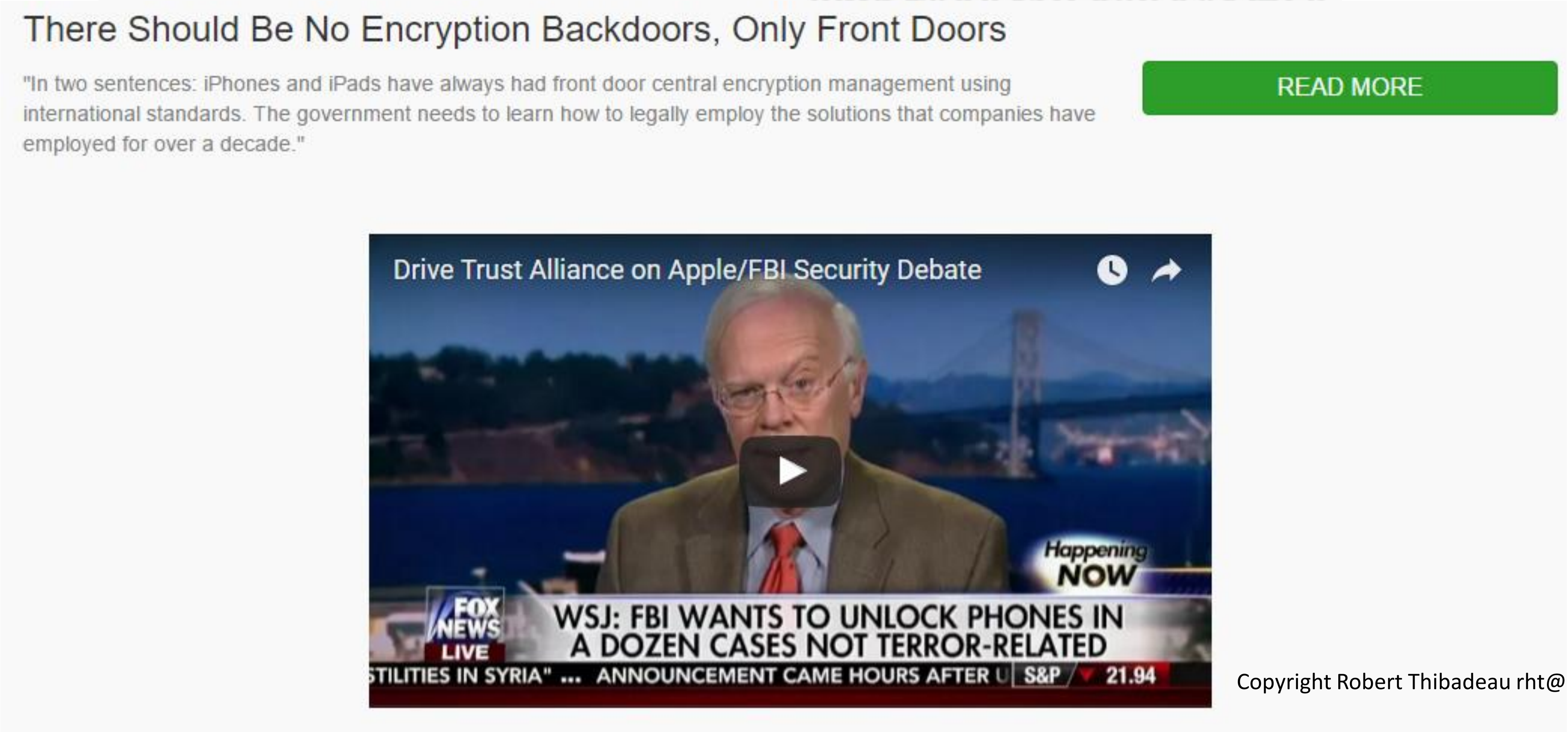
- Open Source code for TCG ***Opal*** and ***Enterprise***, SATA, SAS, NVMe, USB clients (Windows, Mac, Linux).
- Licensable Commercial Products based on our Open Source (Like Red Hat, Inc.)
- Strategic partnering with software contributors (adding to client code base), TCG, and a number of companies.
    - Part of this talk is to get ***some more code for the community***!
    - Part is to ***show how close we really are to consumer adoption*** and the projects we have underway to move SEDs into the fast lane.
    - ***Including IoT***

www.drivetrust.com

A BILLION PEOPLE A DAY USE SELF-ENCRYPTING DRIVE TECHNOLOGY

iPhones, iPads, Android
All of Google etc
All Printers

-- "USER" Data



There Should Be No Encryption Backdoors, Only Front Doors

"In two sentences: iPhones and iPads have always had front door central encryption management using international standards. The government needs to learn how to legally employ the solutions that companies have employed for over a decade."

READ MORE

Drive Trust Alliance on Apple/FBI Security Debate

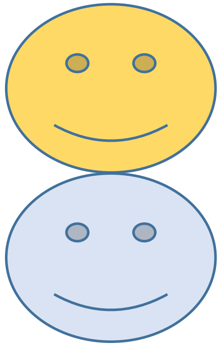
Happening NOW
FOX NEWS LIVE
WSJ: FBI WANTS TO UNLOCK PHONES IN A DOZEN CASES NOT TERROR-RELATED
STILITIES IN SYRIA" ... ANNOUNCEMENT CAME HOURS AFTER U
S&P 21.94

Self-Encrypting Drive Technology for Consumers

☺ Complete protection

☺ Complete invisibility

Consumer Adoption To Date!



- Incredible Adoption to date:
  - ~ 100%: Data Center Storage (e.g., Google)
  - ~ 100%: All SSDs
  - ~ 100%: All Network Office Printer/Copiers
  - 100%: All Apple iOS devices (iPhones, iPads)
  - 100%: All Android Licenses going forward …

  - Mostly for Repurposing : Cryptographic Hiding

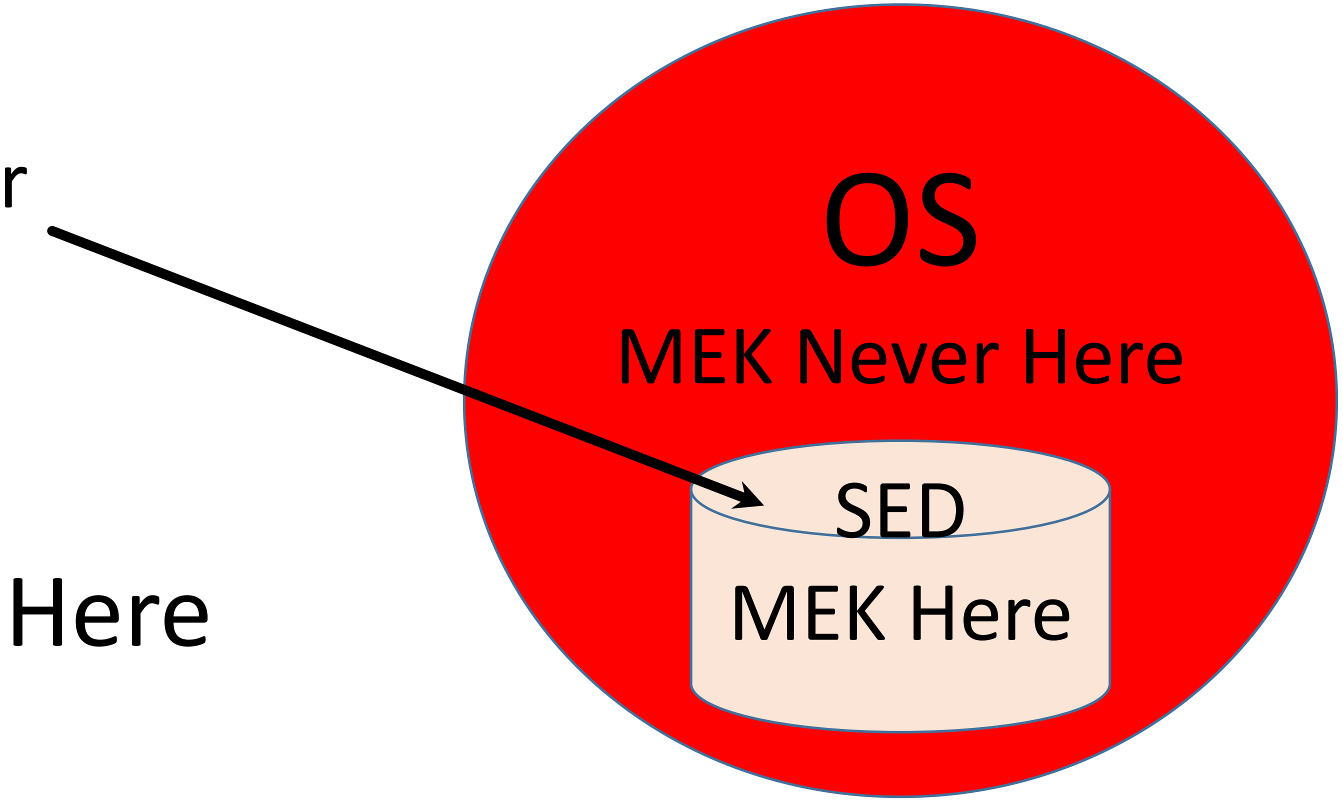
SED Definition & Adoption To Date

- SED == Encrypt-Inline-HardWare-direct to-Storage-Media (KEK(MEK), Data)
  - MEK – storage Media Encryption Key
  - KEK – unlock Key Encryption Key ~= ‘password’

- Cryptographic Hiding works by losing the KEK or the MEK (or both, of course).

What’s an SED?

KEK Unlocker
‘password’



MEK Never Here

No Encrypting or Decrypting Performance Impact

Complete Protection 1 (You can’t get to the data even if you try real hard).

- Data at Rest: That does not mean the power is off…
  - TCG SEDs have range protection. Object storage can have object protection.
  - iPhones have, for years, employed range protection (the system storage is open). Bitlocker eDrive, the same way.
- What this does mean is that when the range is protected, there is no secret (KEK) inside the drive that protects the media encryption key (MEK), that can be known by any amount of engineering (that we know about) inside the drive. (The KEK is just a hash that recognizes the right KEK from outside the SED.)
- In TCG SEDs, the key-encryption-key (KEK) secret that protects the media encryption key (MEK) is 32 Bytes (256 Bits).   If this secret KEK is a random number, the secret will be as strong as the 256 Bit AES MEK.

Complete Protection 2

- The weakness is the KEK (the “password”). Problems:

1. If it is not actually a random number, the strength will only be as strong as the password.
    1. PBKDF2 can hide a bad password because this hashing will spread the non-random bits around in the 32 bytes and make the 32 bytes look random. But this just slows down an attacker in guessing passwords.
    2. Time limits, try limits, self-destruct limits, are the same. Just slows down an attacker.
2. More fundamentally, just using the password once successfully can allow an attacker to do a replay-attack. Whether PBKDF2 or not, he just replays.

Complete Protection 3

- Public Key Cryptography. Key exchange protocols.
    - Including nonce (another random number 32 bytes, generated by drive)
    - Public exchange key can be read off the drive (in an X.509 certificate)
    - Drive (that has the private exchange key) can figure out the password.
    - Replay won’t work.
- But, to do this and maintain protection, you have to protect the KEK in a secure place that knows the KEK and can do the Public exchange key encryption.
    - (There are also other ways to do the key exchange with variants on public key cryptography but the essence here is correct.)
    - Can have both physical presence and remote key splits.
- Phase 3 of the complete protection requires two different devices, one is the SED. The other can be another SED, but could just be a secure computation dongle like a smart card, a web service, or an isolated part of the processor.

Complete Protection 4

- The SED lies. Someone modifies the firmware or hardware in the drive and gets the SED to lie.
- I contributed a method to the Common Criteria process. It basically lets you check by making it hard for the drive to lie. Drives have lots of space and not good mechanisms for hiding computations (in big randomly directed ways). So, you can test a drive as long as the drive can’t know you are just testing and everything looks OK to the drive.

Complete Protection 5

- Without complete protection, consumers will ultimately not like SEDs. Consumers need to believe that their private stuff is (near) perfectly protected…because it is.

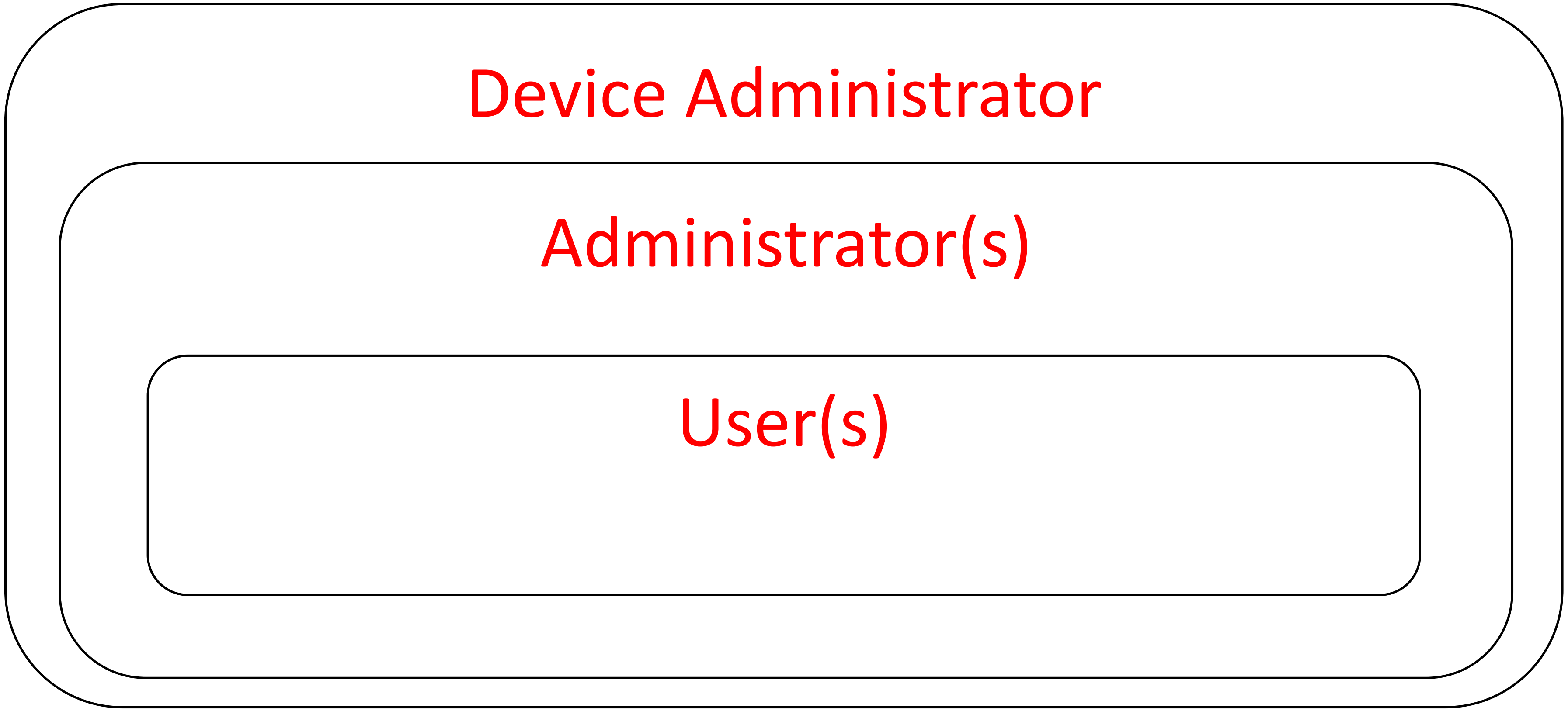
Complete Invisibility - 1

- Examples in Storage networks, Network Printers
  - Basically 100% TCG Standardized, but essentially fully automated for repurposing use case – secret in hardware or server
  - Apple FileVault, Microsoft Bitlocker, even iOS
    - Basically when you log into the OS you have supplied the KEK, and didn’t even know it.
    - Except, you hate to login.
  - Self-Encrypting Box (Demo), like WD USB in that it is password based, but our SEB is not proprietary encryption and is an industry standard.
    - Still, you have to type in a password…or have a secure source provide one and hope it’s not subject to replay

Invisibility 2 : Central Management

- You are seeing the beginning of this today with OAuth and the web. Google is keeping track of you. As is Microsoft. As is Facebook. As is Apple. Etc.
- Ideally, the client machines should be aware of your presence:
  - The Login prompt should disappear forever, and you can get a panic button (which is much more comforting to have around).
  - Fun new software: KMIP for clients. Interesting software that keeps your stuff at rest unless things are safe for you to have it available.
  - Practical applications: BYOD. Containers with conditions for use. See Beachhead Solutions.

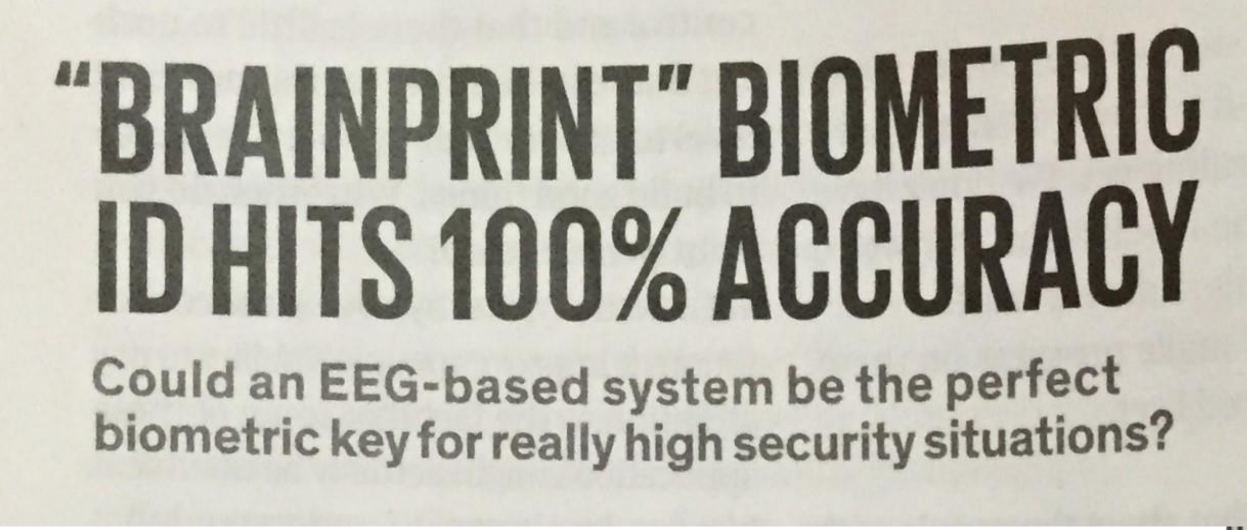
What’s a Front Door?



Invisibility 3 : Trusting the Central Management

- Central management means you now trust a third party or a third party location
  - Hide the credential proofs : Same way they are ***supposed*** to be storing only salted hashes for passwords.

Invisibility 5: Perfect User Authentication : EEG?



“BRAINPRINT” BIOMETRIC ID HITS 100% ACCURACY

Could an EEG-based system be the perfect biometric key for really high security situations?

leagues described in *IEEE Transactio*

ioi-

ns,”

es-

ed

ng

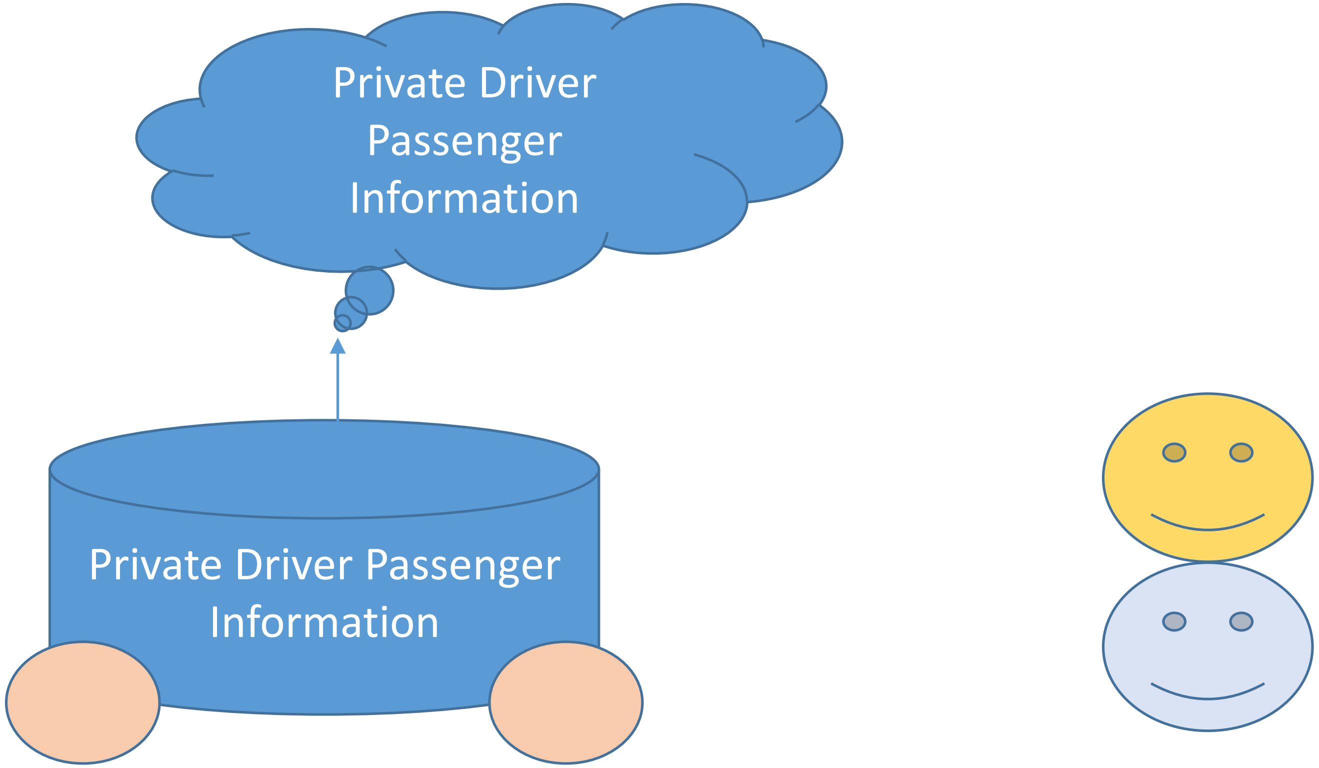
Implantable Public-Key Smart Cards?

Biometric Problem: Can Unimplant (or Make a copy of a fingerprint or eyescan, etc.) Can’t undo.

Invisibility 6: Kaje : Advanced Capability Testing

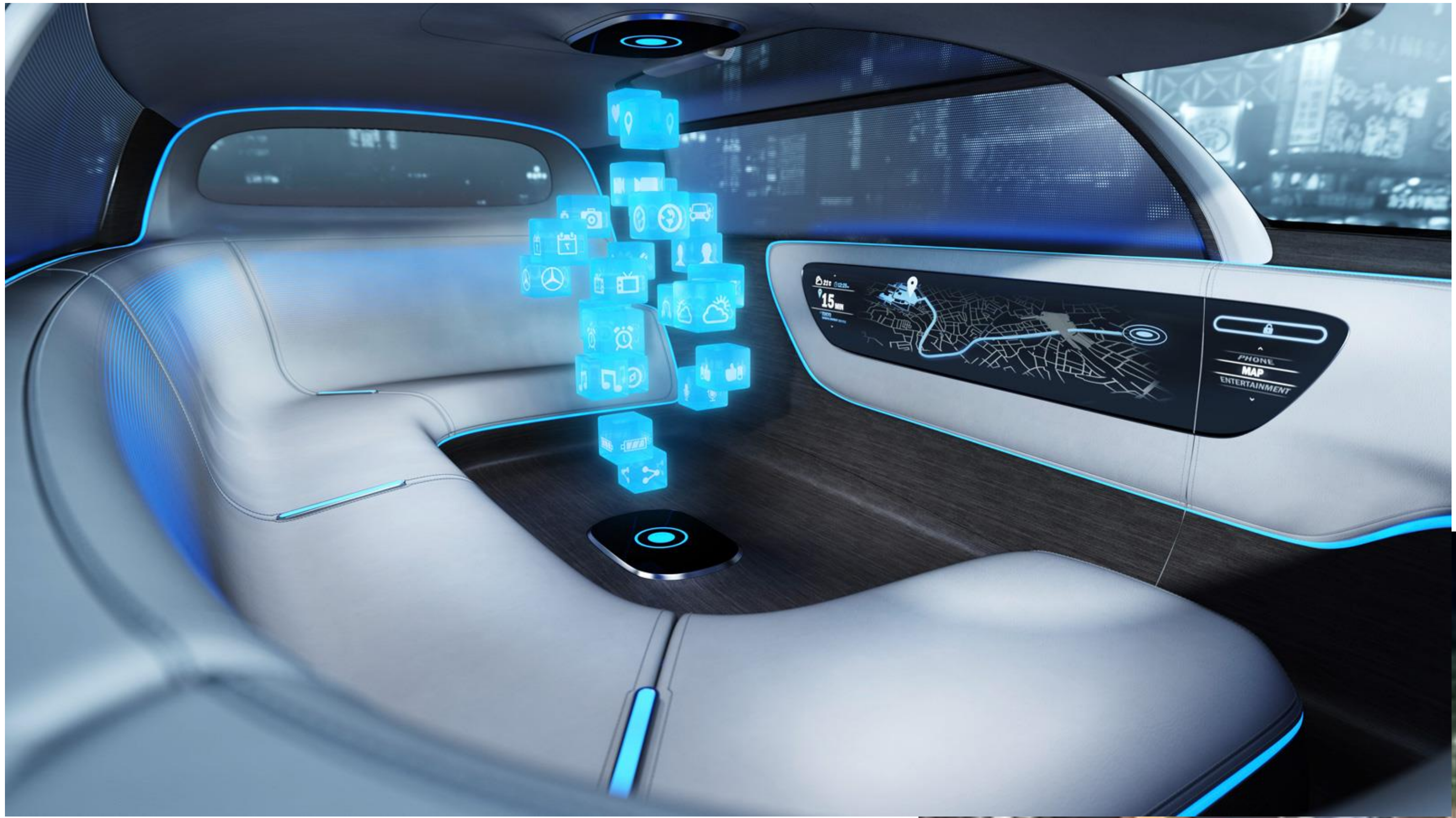
- Cognitive Testing Platform == Publishing Questions with Latencies
    - It’s me (usual authentication problems)
    - It’s really really me and I’m OK
        - Signaling I am lying
        - Signaling I am sure it’s me

IoT Applications (lots, but here’s automotive)



Private Driver Passenger Information

Private Driver Passenger Information



Your Car Web Site Crypto Erases Data (for resale of car)

Your ‘Key’ Unlocks Encrypted Data (for who is in car)

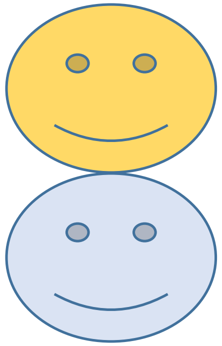
Introducting DTA Self-Encrypting Box
www.drivetrust.com/apps

- Licensable Based on DTA Open Source
- USB TCG Opal for Windows, Mac (later Linux)
  - Includes Micron SED, USB Connector, DTA Consumer and IT Apps
  - Not Proprietary SED (Can always get the data…even years from now).

Desirable Code Contributions

- UEFI Preboot Authentication (currently only supports BIOS preboot)
- KMIP Network Control for remote IT controls
- Public Key for KEK hiding
  - Secure Computation Space on Laptop
  - Or in firmware of SED (TCG SWG proposed CRAM Protocol).

Many Other desirable functions for



Questions?

Bob Thibadeau

rht@drivetrust.com