philip andreae
and associates

PUCHE
Slug
Thing
Mouse
On the Identity Chain

pa

Cando Architecture
An Intuitive Circuit Inside a Slug

Your Interoperable Companion

NFC, BLE, WiFi, GSMA 5G, NFC, 7816, AM/FM, Short band

☺ What Else ☺

Docks with Visual and Audio Local Specific Configuration

CPU, TEE, SE, I/O, RAM,

Crypto Co-Processor, Security & Sensors

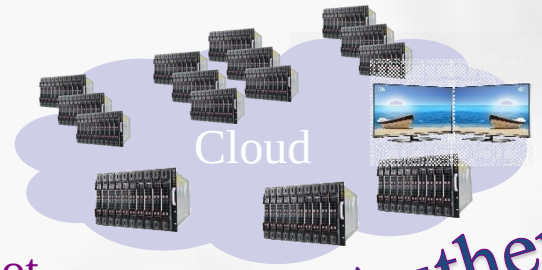
Memory : Flash or E²PROM and ROM

EMV, ICAO, FIDO, PIC eIDAC … Certified Biometric on-board matching and verification NIST AAF=3, IAF=3 EAL3+

AEIPS, CPA, DPass, MChip, VSDC … Domestic, Express Pay, PayPass, PayWave, ZIP, MiFare, CiPurse, Calypso

A Slug Full

Your Credential Guard



☺ What Else ☺

Authenticator

Hotspot
Microsoft Office
Calendar, contacts & email
Directory server extensions
SharePoint &
One Drive

Your Identities
My Relationships
My Skills
My Certificates
My Attributes
My Data
My Secrets

CPU, TEE, SE, I/O, RAM

Crypto Co-Processor, Security & Sensors

Memory : Flash or E^2PROM and ROM

References and bound to & in the chain

The Marble

Primary

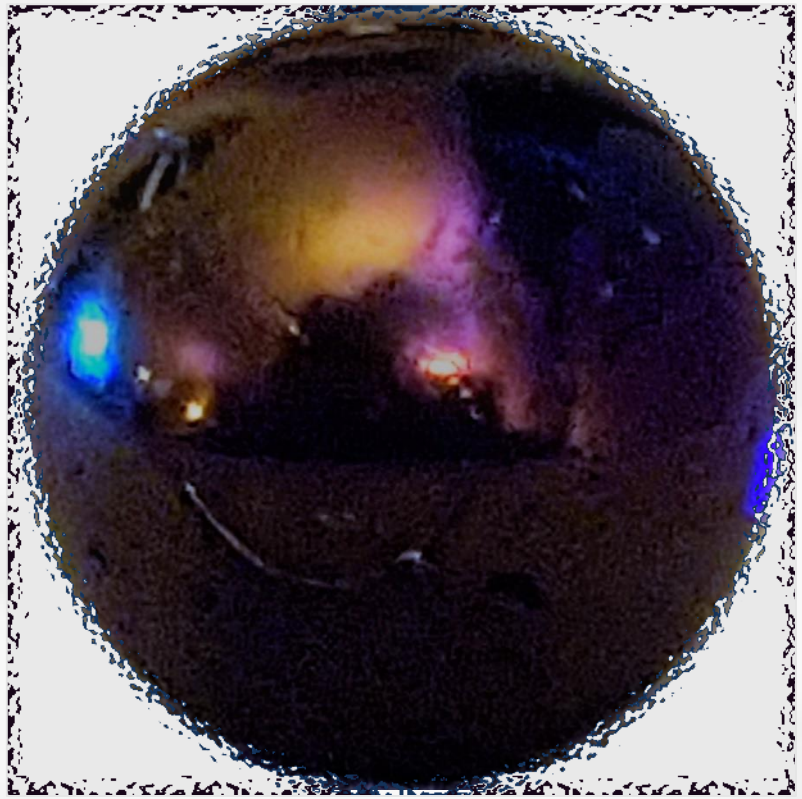
- Pairs to Secondary
- Pairs to Headset
- Pairs of Slug (VPN)
- Genesis Block

EKG

One to One Matching

Will pair to other Fitness M

Multi-layers of “What you Are & Have”



Secondary

- Pairs to Primary
- Pairs of Headset
- Pairs to Slug
- First Consensus event

Pulse

Prepared for Exportin Centralized Schema

Collects and records

Multi-layers of “What You Have” w/ “What you Are”

The Intuitive Thing

Durable

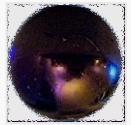
- It is designed with a 10 year life.
- Extensions to experiences at engagements

Secure

Break it, smash it

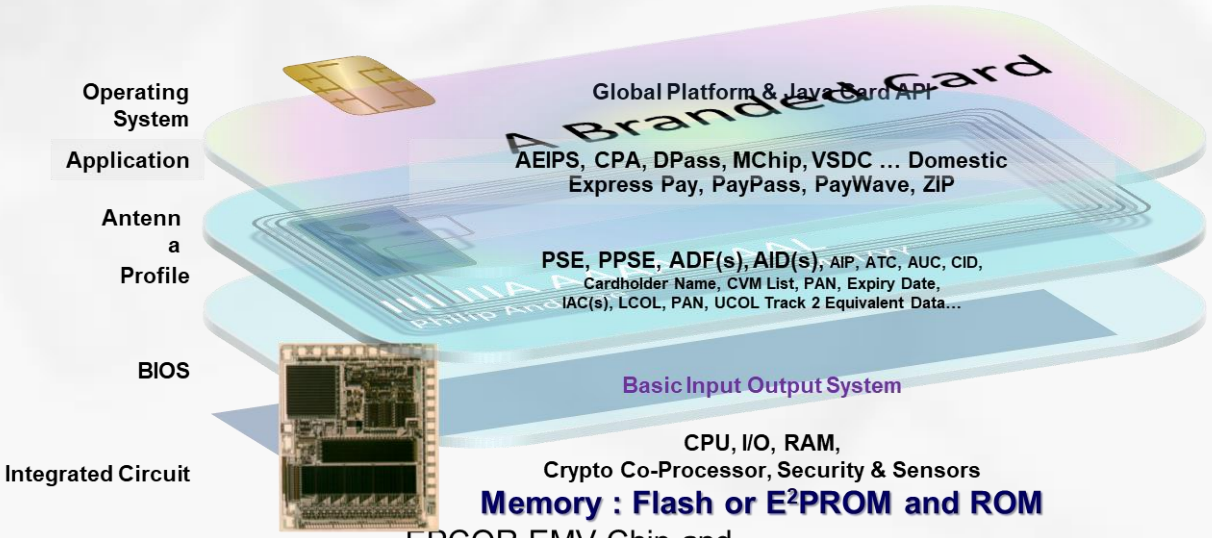
interrupt it

Its gone



philip andreae and associates

Offering the Dip or Tap Feeling



EPCOR EMV Chip and Choice 2018

EMV the Global Standard for Credit & Debit Payments

EUROPAY International
MasterCard Worldwide
VISA

In 1993 The International Payment Brands Decided The Long Term Solution To Fraud Was The "ICC"

We Agreed To Develop A Common Specification To Assure Global Interoperability

We agreed the requirements and published "The Integrated Circuit Card Specifications for Payment Systems"

EMVCo is owned & staffed by Visa, MasterCard, JCB, American Express, UnionPay and Discover

Counterfeit Protection
Off/On-line Authentication

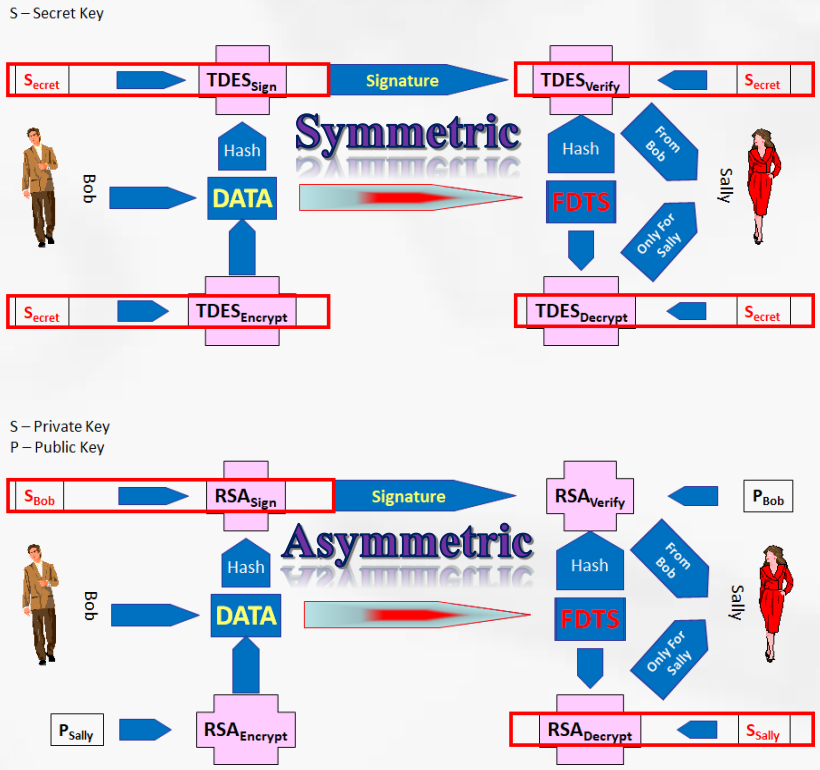
Lost and Stolen Fraud
Cardholder Verification

EMVCo

Offline Authorization
Cost Reduction

Revenue Creation
Value Added Services

At Its Core
What You Have Is An Integrated
To Assure Your Identity
What You Need Is A Secure Element Inside



- The chip on a card
- The TPM in most personal computers
- The secure enclave in an Iphone
- The secure element inside many devices
- The TEE in most phones
- The HSM on most hosts

The IC employs cryptography
To securely store and execute using:

- Secret Key(s)
  Triple DES, AES … Online authentication
- Public / Private Key Pairs(s)
  RSA - Quantum Offline authentication

FIDO & NIST 800-63-2 AAL-3

FIDO, W3C, WebAuthN & WebPayments, Automotive, Home, City … Health

What You Have
A Secure Element Inside

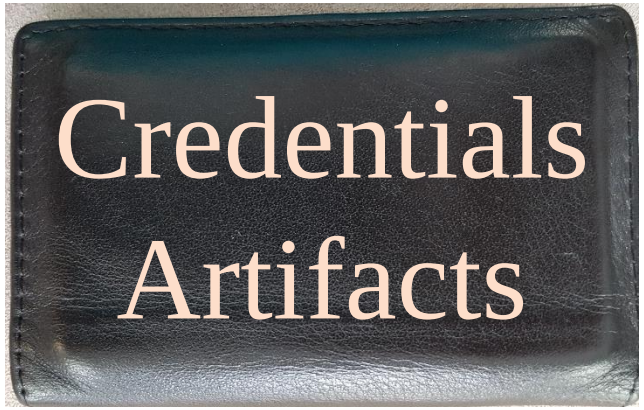
IATA – International Air Transport Associations PSE – Payment Systems Environment ICAO – International Civil Aviation Organization

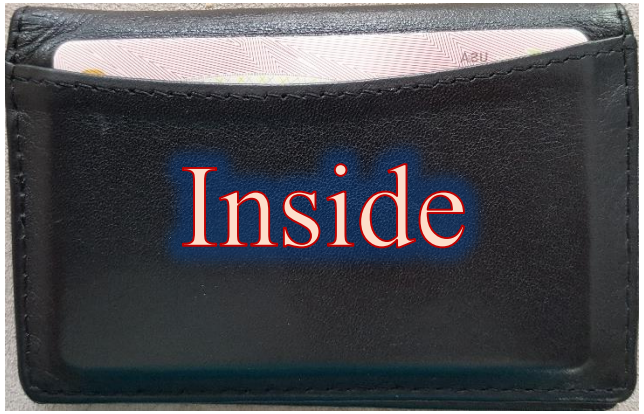
Payments	IATA	Enterprise	Loyalty	Gov't ICAO	Health	Home Auto	Member
Credit Debit Stored Value Transit Card	Ticket Itinerary Boarding Pass Frequent Flyer VIP	Identification Physical Access Logical Access	Points Rewards Coupons Discounts	Passport National ID Drivers License Birth Certificate National Health	Health Insurance Physician's Details Emergency Data: Blood type Donor	Home Security Car Keys Library Card Home Address Passwords	Fitness Club Library Card

KEY USES

Data Storage, Digital Signature &
Electronic Purse, Certificated, Access

Identification, Authentication, Verifications





CanDo Designed to do for you. It learns as you register. It recovers like you did. Optimized from learning. It is your authenticator.

The

blob, slug, fob, card - Thing

CanDo Designed to do for you. It learns as you register. It recovers like you did. Optimized from learning. It is your authenticator.

The Thing The object at core to your security. Is in any shape you can afford to build. **It adheres to standards** **We** test to be certified to anything! Others can design whatever they want as long as they adhere to the standards for the situations they contemplate interacting with. Collectively working with the goal of global interoperability in all means of desired communications and engagement.

1997 I met Unicate
We almost had a solution

Mobile Payments

NFC (ISO 14443) – In the Mobile phone

« SIM *Centric* » *model*

Removable
Authorises the access to the Telecom Operator Network
Standardised technologies
The MNO is the Secure Element issuer and owner

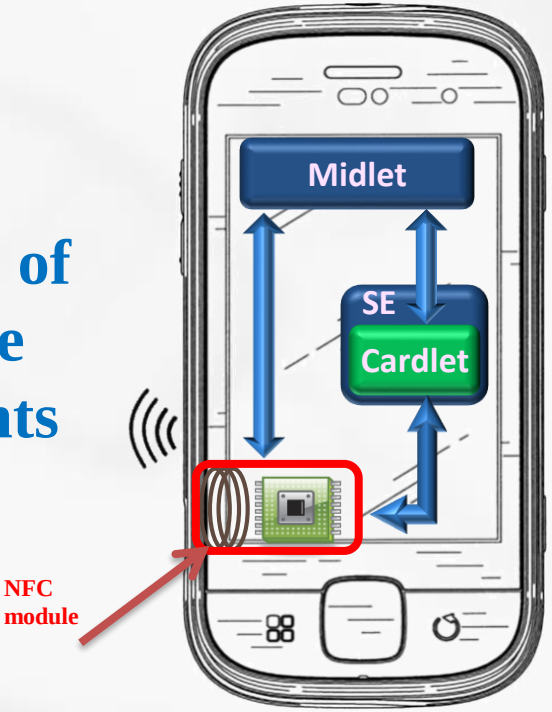
"Embedded SE" model

Unmovable
Few compatible phones
Proprietary technology
The MNO, is the issuer and owner of the SE

Host Card Emulation (HCE)

The Secure Element is in the Cloud
The Application can emulate a Card
Disintermediates the MNO and OEM

3 Types of Secure Elements



SE-Secure Element: secure platform, hosting the application
Cardlet: payment application embedded in the SE
Midlet: GUI-Graphical User Interface for the payment application; installed on the phone

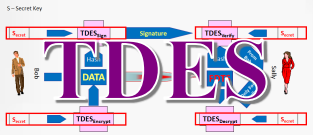
Three Factors Define The Chip & The EMV Profile

Authentication

"What you have"

Offline at Merchant (RSA)
Requires RSA Capable Chip

Online on Issuer Host (TDES



Signature

Verification

"What you know"

PIN as CVM – Match In Chip
Required if offline authorization is supported

On Host PIN
No CVM

Authorization

"You have the funds"

Offline

*Uses **Issuer Defined Card Risk Management Parameters***
Requires Offline Authentication

Online
Issuer Host Authorized

The Key to Secure Identification
Multi-Factor Authentication

➢**Something You Have**	✓ The Token	**Card/Phone**
➢**Something You Know**	✓ The Secret	PIN/Password
➢**Something You Are**	✓ A Biometric	**Physical Behaviors & Attributes**

1236!S*97ally
1237!Sally
9866!Sally
9876!Vally
S>lly!1236
Sally!1237
Sally!9876
Sally!9&%6
65$q8@aM
75$q8@aM
7$nR6&zZ
6$nR6&zZ
6$nR6&zZ
*8G%h67#aW
Pas*wor&
Passwor&
An&reae
Andreae
A&min
Admin
Pan&reae
Pan&r$ae
*8G%h67#aW

Layered Security To Assure Identity

EMV, PIV, ICAO eID, FIDO …

User Name, Phone Number
As The Identifier

Hardware Secured Secrets
Biometric Sensors
& Power of Cryptography

A Biometric Authenticator
Assuring You are You

The

blob, slug, fob, card - Thing

CanDo Designed to do for you. It learns as you register. It recovers like you did. Optimized from learning. It is your authenticator.

The rest of your interaction is about communicating with reliable parties and strangers

In an insecure realm of villainy

It is a wide west in the land of digital make believe.

Authentication is the key to digital security

Verification merged the various factors to match risk

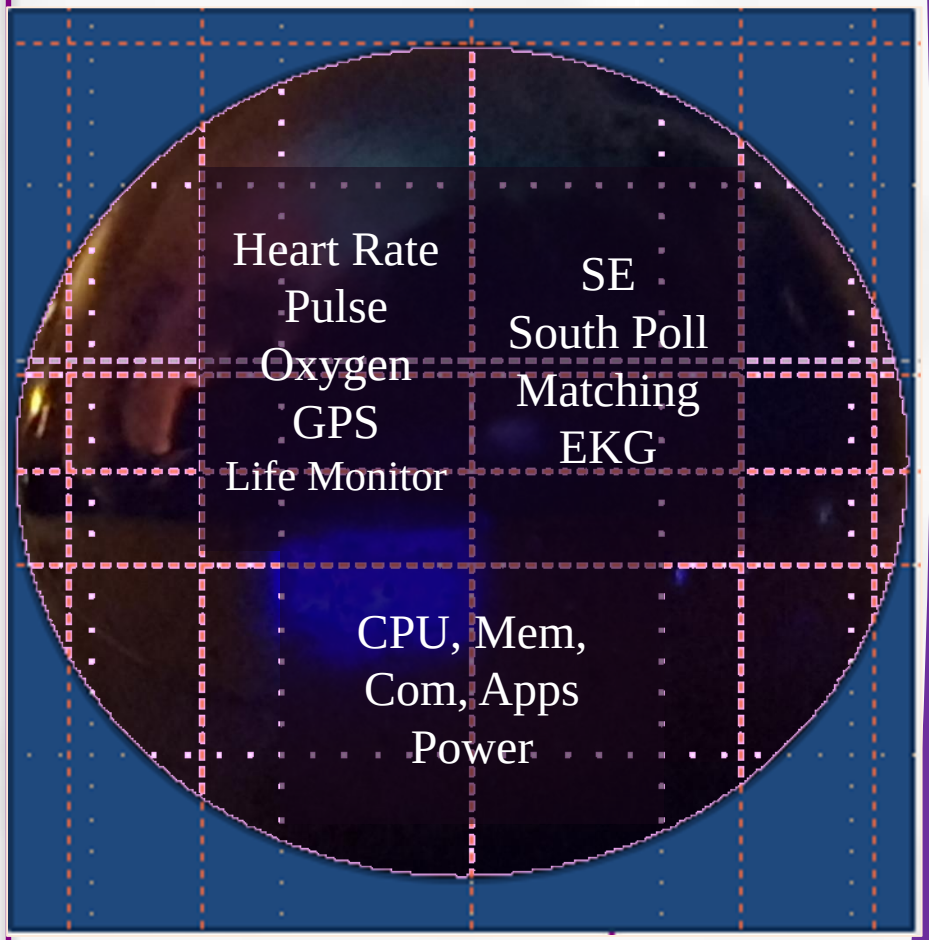
Smart Card Solutions Require a Reader.

1996
I met Unicate
We almost had
The solution

The Marble

Two authenticators are required to register in Recovery. The Marble is the Source. Don't lose it before we get the next device turned on.

- Marbles
- Authenticator(s)
- Three The magic number
- For each Recovery Identity
  One Coin is issued
- Pair to user interface
- Pair Two Marbles
- Pair Marbles to Slug
- Pair w/ Watch
- Pair w/ Car



Business Model

Seed from the top and the bottom (entitlement)

- 0ne Million
- 0ne Billion

Focus on luxury implementations

FOCUS ON THE MY OF IDENTITY

Define and make sure sufficient players operate as validation nodes.

Catalog the Standards

Provide the best practice implementation

Administer Certification

Bottom & Top

Basic system

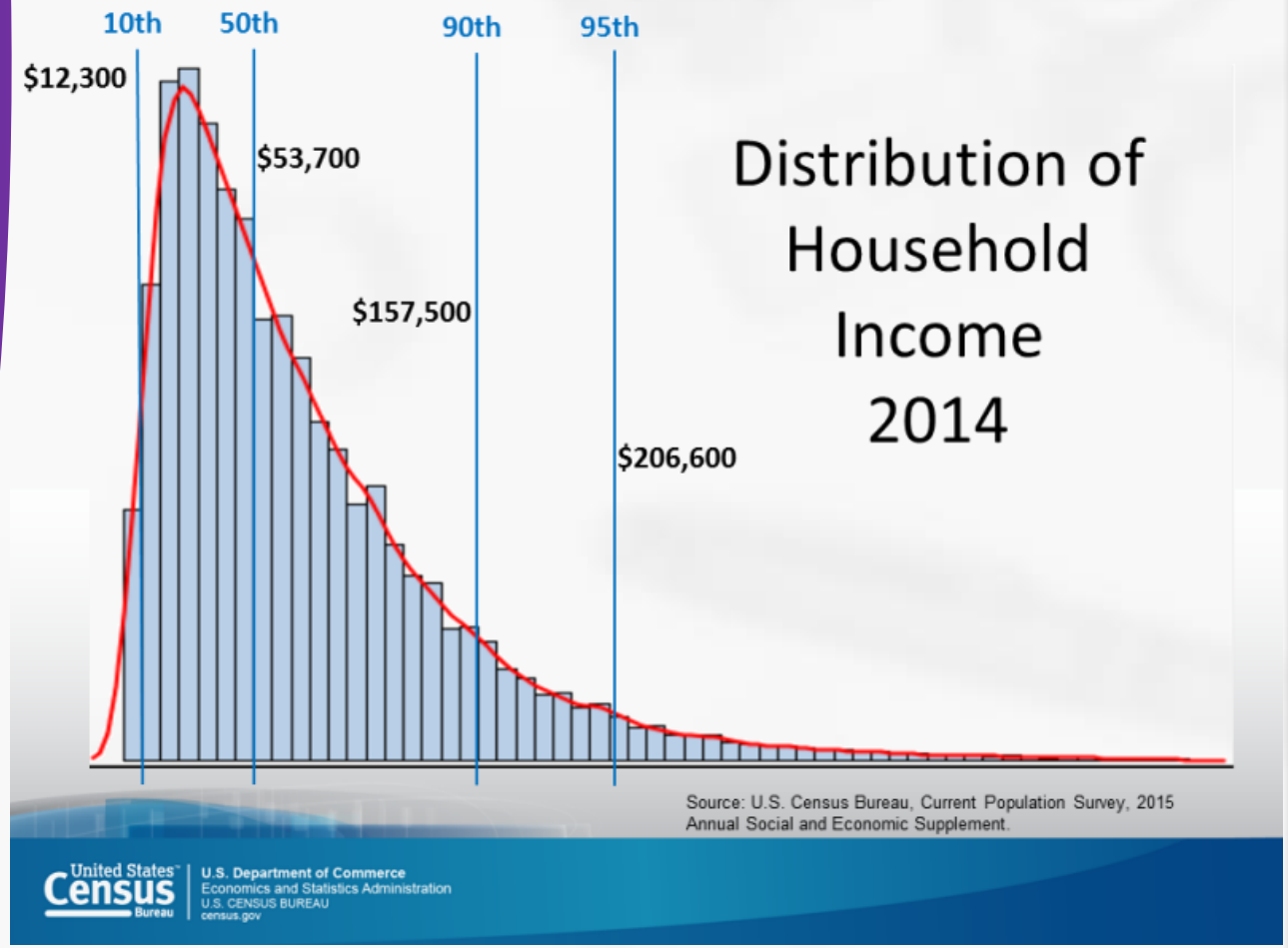
1. **Dual interface card PVC**
2. **14443 Antenna Inlay**
3. **RSA Dual Interface ICC**
4. **Embossed and encoded**

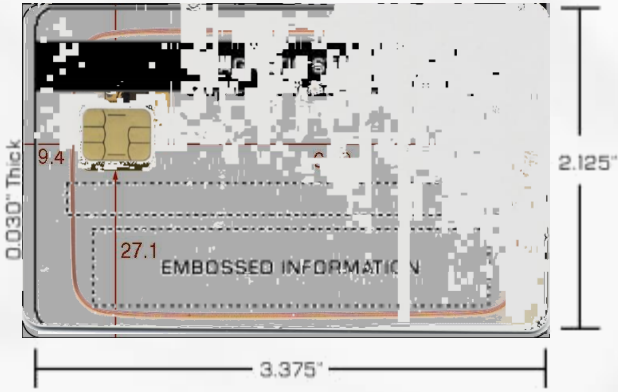
The Brick

- **Virtual Screen**
- **5 ID-1 deep**
- **Card Recharger slot**
- **HDR WQHB+ Front display**
- **E-Ink Back Display**
- **.5 Tera Byte**
- **PIN Pad - EPP Certified**
- **EMV, Payment apps, ICAO, PIV, MAP, Excel, PowerPoint, Word, eMail, browser … APPs**
- **5G-GSM, WiFi, BlueTooth, POTS, GPS Sensors**

Addressing The Needs of the Many

The Billion





Base Stations Afford Connections

- ✓ The Front is a Ultra High definition Screen, with touch, behind the glass fingerprint, sensors, cameras, mic array, hotspot, GPS, WiFi, NFC
- ✓ Intuitive device based data, matching, authenticator, verification and everything else
- ✓ With secure cloud for extensions & virtualization

philip andreae
and associates

Any Questions

Philip@Andreae.com

www.andreae.com

philip andreae
and associates

Any Questions

Philip@Andreae.com

www.andreae.com