

INTER-REGIONAL STANDARDIZATION FORUM FOR BRIDGING THE STANDARDIZATION GAP (BSG)

Muscat, Oman, 11-12 December 2017



Arab ICT Organization
(AICTO)



Information Technology
Authority
Sultanate Of Oman



International
Telecommunication
Union (ITU)



African Telecommunication Union (ATU)



National Digital Certification Agency
Tunisia

Reputation-fortified E-trust: Blockchain, PKI and IoT

David W. Kravitz, Ph.D.

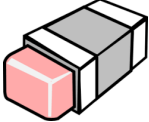
Vice President – Crypto Systems Research, DarkMatter, UAE

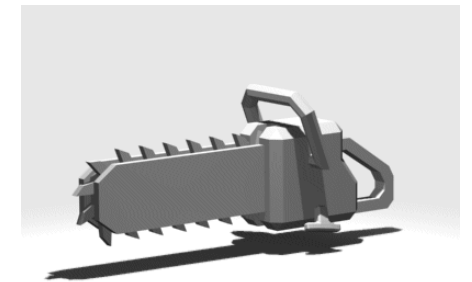
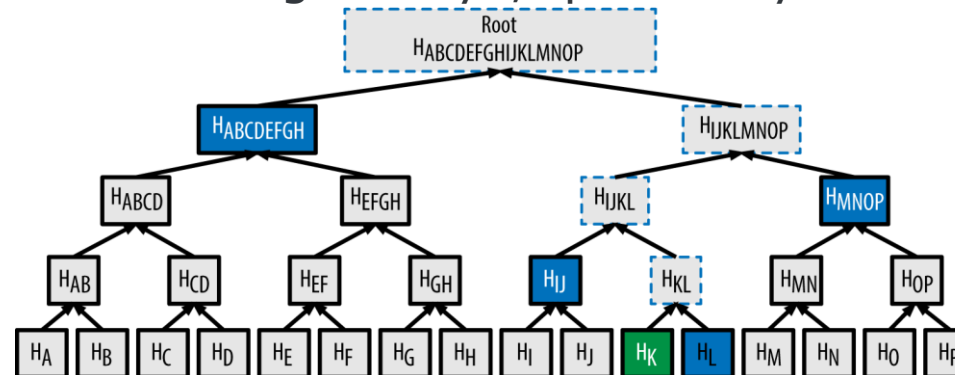
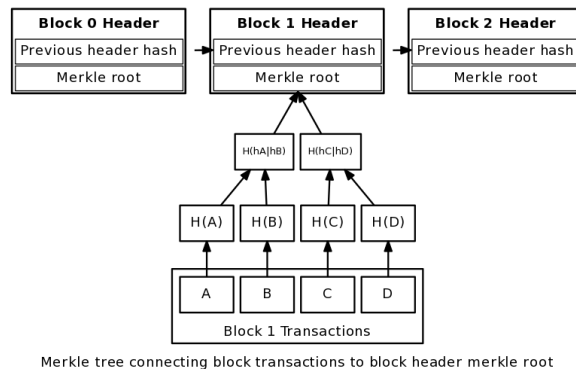
Blockchain: mining for gold- or pixie- dust?

- Fortune.com: email from Vint Cerf, Chief Internet Evangelist at Google (coauthor of TCP/IP)

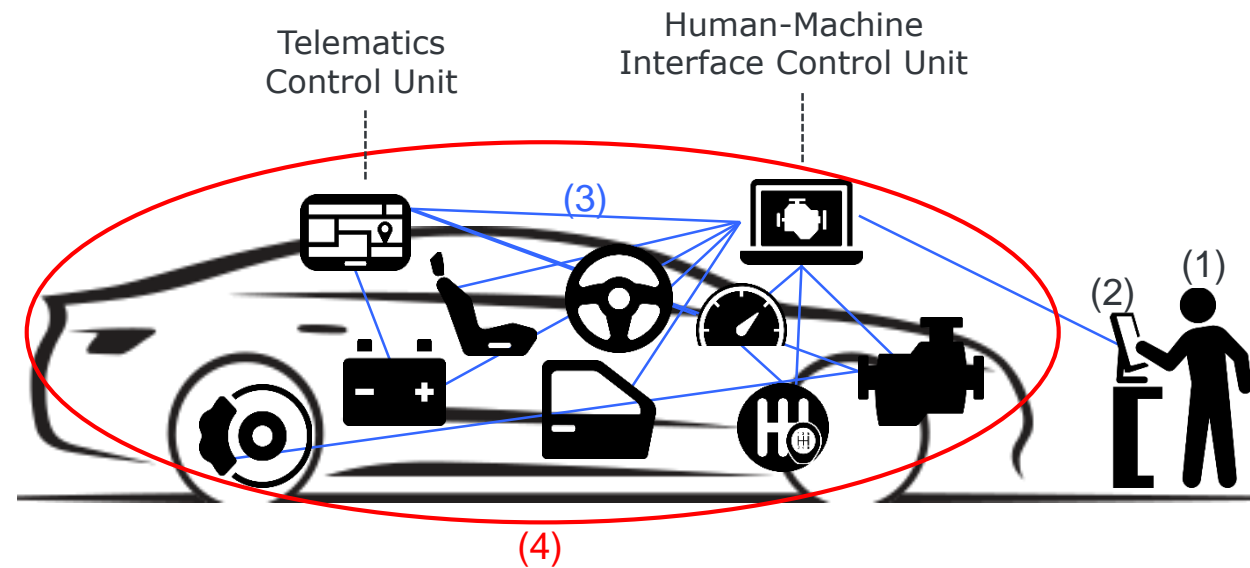
“It has become a kind of magic pixie dust for some proponents.” Still, even Cerf sees potential in blockchains, where “the parties involved in the system are known and can be evaluated for reliability and trustworthiness.”



- GDPR:** right to be forgotten  ; offloading access to sensitive assets
- Coindesk.com: **Will Provenance Be the Blockchain's Break Out Use Case in 2016?**
- Full nodes, pruning, and light nodes: IoT gateways; queries by resource-constrained nodes



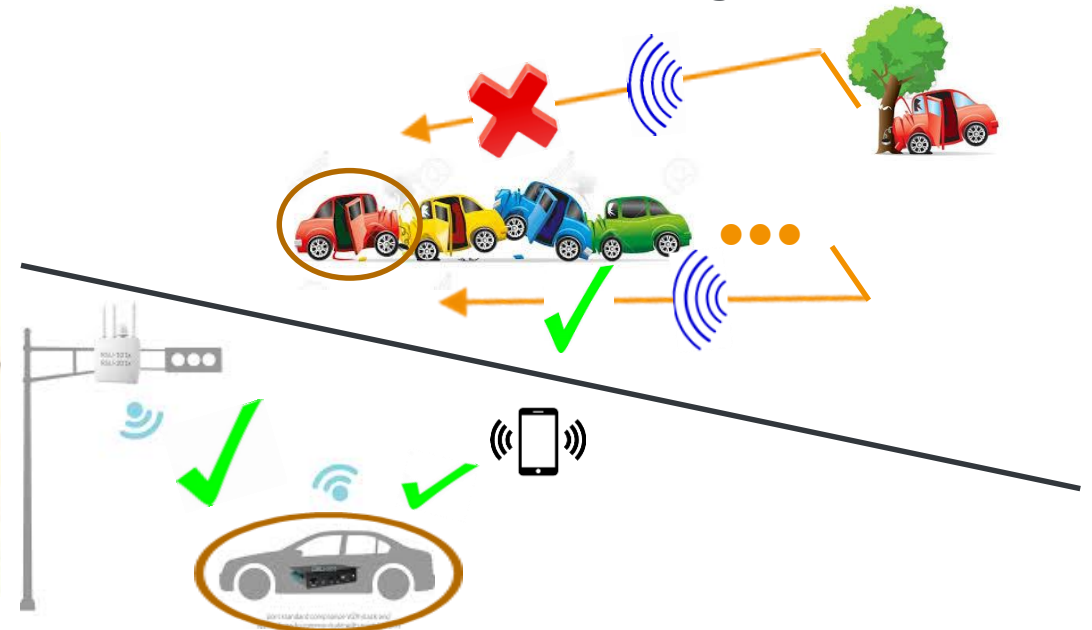
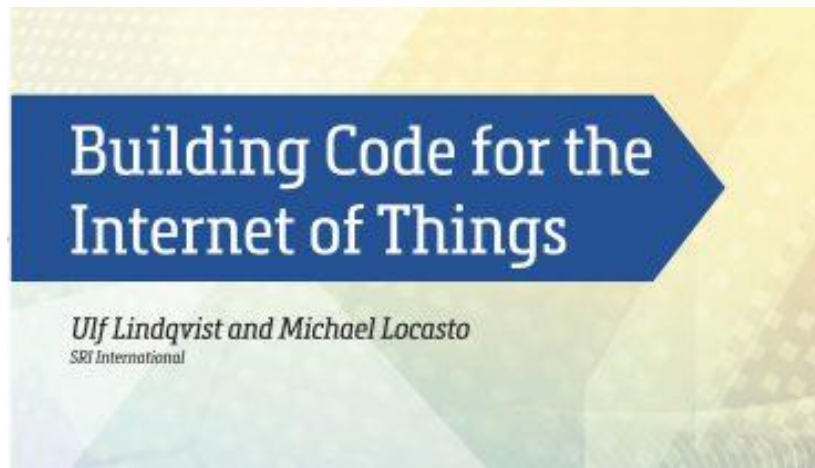
Installer establishes secure communication lines between IoT devices (Electronic Control Units) in a vehicle



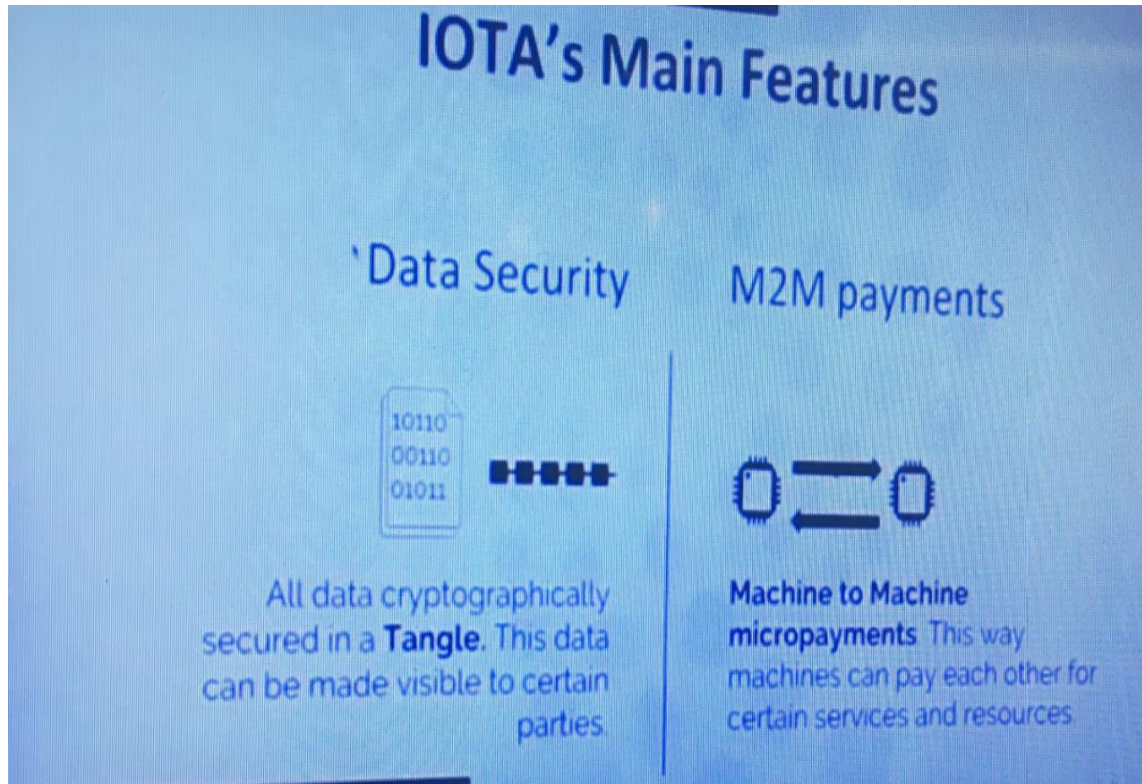
**The IoT devices within the vehicle
become members of an “IoT Devices
Group”**

Isolation boundary – context – getting to know you

“Even in the case where isolation boundaries are well-defined, complete, and sufficient to protect a system or component against compromise, interacting IoT systems might require well-defined ways of adjusting this isolation to access parts of another system (for example, in the case of a smart cities subsystem compensating for another during a natural disaster). The decision process governing this adjustment of the isolation boundary needs to be able to gauge the context of the situation and the trustworthiness of the entities being considered for inclusion inside the boundary.”



Caring more than one iota



- Dominik Schiener, Co-founder of IOTA Foundation:
17 October 2017

Major underpinning of IOTA: Transaction submitters actively distribute to consensus by validating transactions – “We truly believe that permissionless innovation is going to be the key component of distributed ledgers.”

“A transaction in IOTA can contain two things...Either it can contain value...and the 2nd component is all about data security.” “IOTA is the perfect protocol when it comes to data security.”

“The main reason why IOTA is really, really awesome is because we have no transaction fees.”

“...protocol doesn’t really care what type of data is transferred.”

“What I’m really worried about is how do we go away from permissioned ecosystem towards this whole permissionless ecosystem.”

“... and the beauty of IOTA is -- because it is so lightweight -- it can all work in the browser.”

Is the system secure?: applying the full “battery” of tests

- Bitcoin supplies partial 1st “A” of the three “A”s
 - Data integrity without entity Authentication
 - a great fit for **ransomware payments**
- Towards “AA”: Full Authentication does not imply Authorization
 - Critical for permissioned blockchains
 - application-specific read and write access policy enforcement
- Towards “AAA”: Managing Accountability
 - Real-life application requirements
 - private and auditable

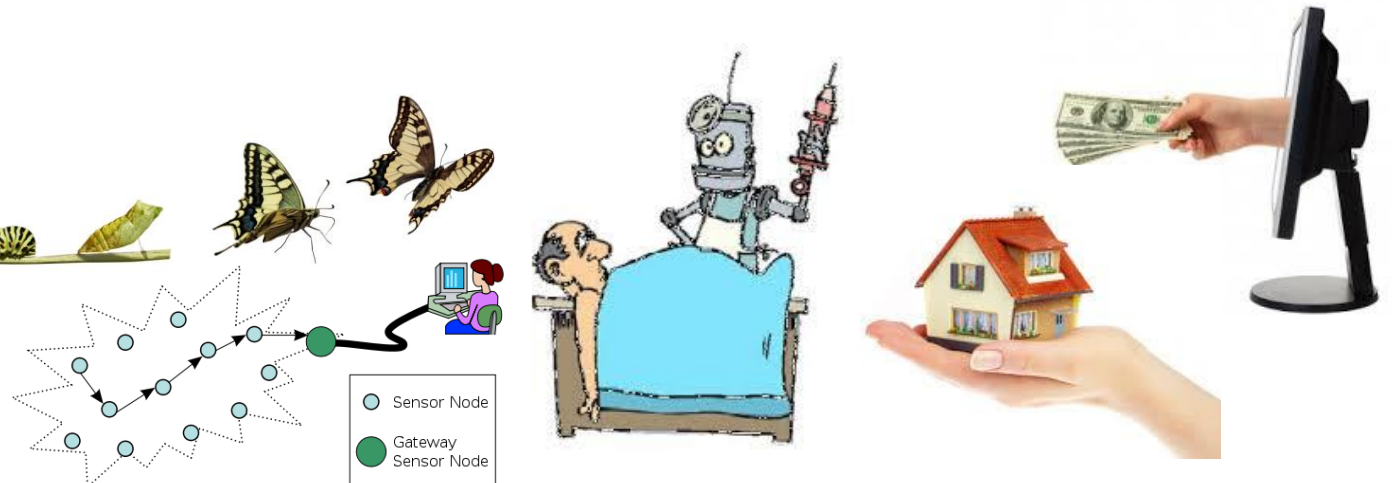


Standards-based with a V2V origin

- NIST Special Pub 800-63B **Authentication & Lifecycle Management**: "The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator."
- NIST Special Pub 800-63-3 **Digital Identity Guidelines**: "A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known. Identity proofing establishes that a subject is who they claim to be."



https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf



Trusted transactions require trusted provenance

Behind the scenes:

1. Static: Standard public key certificate \supset Bob's identity and/or affiliation || Bob's public key; sign fresh assertion request to Identity Provider (IdP) using Bob's corresponding private key
2. Dynamic: Standard (keyless) attribute certificate \supset Bob's attributes || Bob's public key certificate ID; sign fresh assertion request to Attribute Authority (AA) using Bob's corresponding private key

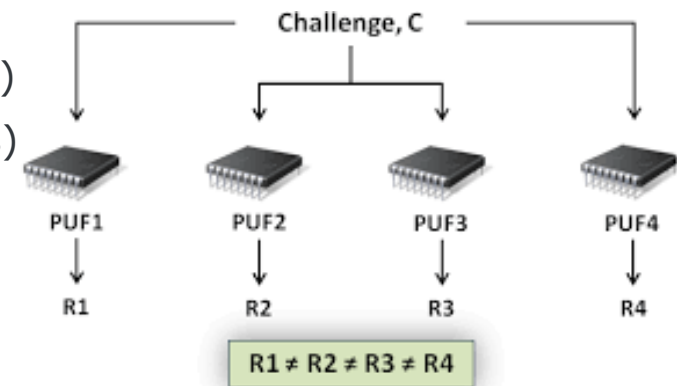
Or

Use resource-constrained device mechanism, such as challenge-response physically unclonable functions (PUF)

3. Convert IdP- issued assertions to uniformly-constructed Enrollment Certificates (ECerts)
4. Convert AA- issued assertions to uniformly-constructed Transaction Certificates (TCerts)

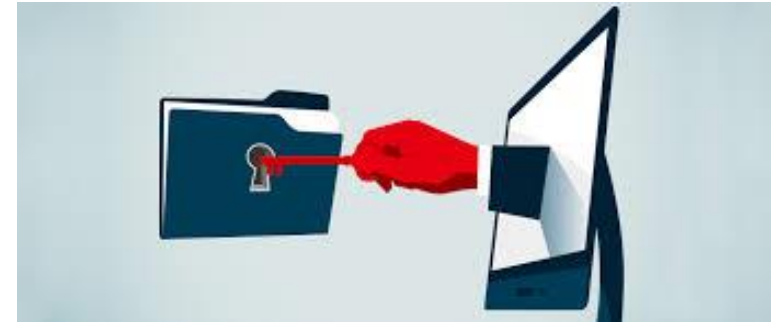
Transaction Certificate \supset Bob's attributes [encrypted*] || Bob's one-time-use public key

[Later: *TXN metadata includes selectively released keys]



Making the blockchain accessible

- Signature TCert- owner:
 - key expansion to recover TCert private keys (signature; key agreement)
 - selective disclosure keys for TCert attributes proof-of-possession (PoP)
- Key agreement TCert- requestor:
 - certain of its PoP keys
- Primary TCA:
 - threshold-/multi- signature generation of TemplateTCerts
- Subordinate TCA:
 - generation of TCerts (redundant & restricted operations)
- Audit₁:
 - capability to cluster transactions for subset of TCert owners
- Audit₂:
 - passively access PoP keys for subclasses of users/devices
- Audit₃:
 - Pre: payloads via Validator-enforced transaction-creator audit granting
 - Post: payloads via key agreement TCerts or authorized queries



Crypto-agility and hash chain migration

- Eventual consensus-driven re-hashing of entire transactions into hash-chained blocks using next-generation algorithm
- Integrity of past transactions maintained
 - Attempted substitution fails even if original signature scheme and its underlying hash now vulnerable
- Confidentiality of past transaction data maintained even if original key agreement scheme now vulnerable
 - If current signature scheme robust and signed query by authorized requester required to access ciphertext
 - Such particular data ciphertext stored off-chain and referenced on the blockchain by its hash
 - Keeps blockchain reasonably sized
 - Consistent with hashing state into transactions

Making



agile:



Network-edge anomaly detection is only as good as trustworthiness of end-entity users and devices

- Subsets of validated, time-stamped, immutable transactions propagated on blockchain can later be released by users
- Supplies evidence of whereabouts and behavior that is not spoofable (even by fraudster using misappropriated PII*)
 - When and where user's devices were or weren't present
 - Veracity of devices attested/corroborated/contradicted by neighboring devices/users
- User reputation / device reputation reflected as attributes or as attribute qualifiers: selectively releasable (publicly, or confidentially to Validators and/or intended transaction recipients)
 - Reputation thresholds may be set by use-case- specific policy as enforceable by Validators
 - Such reputation thresholds may apply to signature TCerts (transaction creators) and/or key agreement TCerts (transaction recipients)



*



Identity and reputation feedback loops

- Trusted users; trusted devices; users trusted based in-part on use of trusted devices
 - Multi-factor authentication:
 - devices owned/operated directly by user
 - assertions/voting/corroboration by (time- or space-) neighboring devices
 - device-based roots of trust, e.g., manufacturer provenance; PUFs: key / random nonce generation, memoryless repeatable-key storage, device authentication, anti-counterfeit
 - Client-server splits:
 - server-authorized dynamic transformation of client that is differentially detectable from adversarial modification of client: through client responses to server challenges
 - server-based dynamically refreshed locking/unlocking of client-local key store modules
- Inviter-Invitee protocol runs: endorsements via attribute certificate chaining incorporated into resultant “communication lines”; initiate “communication lines” as inspired by positive experience with pair-wise / group-wise blockchain transactions, and consider current reputation of potential invitees
 - Invitees can check current reputation of inviters as condition of acceptance
 - Dedicated “communication lines” as prerequisite to entrusting with properly handling sensitive data, and/or believing data (prior to precipitating user action or device reconfiguration/recalibration)
 - Performance metrics of established comm lines affect reputation of participating users/devices

Scalable hybrid transaction model

- Example: On-chain physician order to activate IV apparatus
 - IV apparatus does not wait for and may remain oblivious of payment aspects
- Secure, non-hacked IoT device will not report service fulfillment ahead of actually providing such service (e.g., life-saving IV drip)
- Payment for (single or aggregated) service can be via cryptocurrency or off-chain- reconciled monetary exchange
- Reputation metrics, as incorporated and updated into TCerts, play a vital role in enabling a highly scalable and responsive concurrent- or post- service-delivery payment reconciliation model
- Reputation of devices; reputation of users
 - Device robustness
 - Payment timeliness
 - Service performance timeliness and accuracy
- Reduce dependency on complex fully-automated, non- fully-vetted/understood “smart contract” code

Add an internal Attribute Certificate Authority (ACA) (1 of 2)

- The ACA interfaces with internal/external Attribute Authorities (AA) indirectly via a User Agent that enables the User to acquire verifiably fresh evidence of attribute ownership
 - Such evidence gets amalgamated into an encrypted database accessible by a Primary Transaction Certificate Authority (TCA) for ultimately establishing the legitimacy at Subordinate TCAs of requests for Transaction Certificates (TCerts) that include specified attributes
 - *There may be multiple Primary TCAs that serve a given chain, with overlapping or disjoint coverage areas (such as Affiliations or other attribute types) for which they are trusted by some subset of relying parties. The ACA may encrypt accordingly, so that a particular Primary TCA only accesses attribute ownership proofs within its domain*
- This is analogous to an internal Registration Authority (RA) that interfaces indirectly with internal/external Identity Providers (IdP) in order to apprise an Enrollment Certificate Authority (ECA) of legitimate requests for Enrollment Certificates

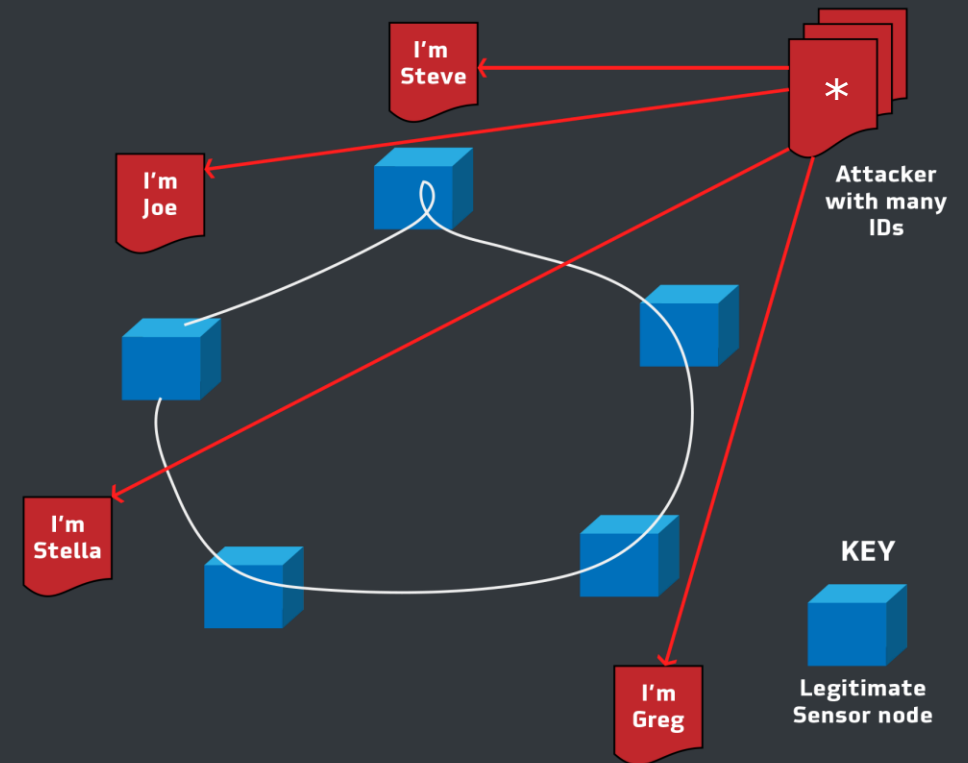
Add an internal Attribute Certificate Authority (ACA) (2 of 2)

- Use can be made of standardized methods such as mutually authenticated TLS, X.509 self-signed (User Agent) client certificates, and SAML holder-of-key assertions
- The combined Public Key Infrastructure (PKI) / Privilege Management Infrastructure (PMI) system may deploy intra-chain, inter-chain, cross-certification, multi-signature, and/or stealth multi-signature (i.e., threshold signature) elements for efficient decentralization that preserves interoperability with legacy/external systems in order to inherit/establish and maintain trust
- Enables a natural split of Client between User Agent and Signature Service Provider
 - hash(Rand) used as an index for TemplateTCerts, where Rand from ACA known only to legitimate User Agent
- *The bootstrapping of identities and attributes through means of PKI and PMI can coexist with web-of-trust- type attestations. As a degenerate case, static and/or dynamic attributes are introduced into the blockchain with 0-level assurance/reputation, such that their lives begin on the blockchain*

An M2M use case

- **APPLICABLE TO AD HOC COLONIES OF DEVICES**
 - Can organize for task fulfillment
- **CALLS FOR DEVICE PARTICIPATION VIA BLOCKCHAIN**
 - May specify acceptance criteria: minimum attribute rating scores
 - Responses by qualified devices are incorporated into blockchain
- **DEVICES CAN USE FACTORY-PROVISIONED CERTIFICATES**
 - Prove attributes to ACA via AA-issued assertions
- **OFF-CHAIN FULFILLMENT**
 - Response transaction TCerts usable for TLS authentication
- **ON-CHAIN MUTUAL RATING OF DEVICES**
 - Reference rated device's TCert
 - Ratings encrypted for access by Analytics Processor (AP)
 - AP clusters individual ratings according to deviceID
 - AP acting as AA issues (cumulative) attribute rating assertions
- **EXTENSIBLE TO H2M**
 - Device matches?: (a) presence at establishment/service use, and (b) user's rating of it when-/where- ever
 - AP clusters TCerts according to owning user, even across multiple devices
 - Thwarts Sybil attacks*

External Attribute Authority (AA)
Internal Attribute Certificate Authority (ACA)



Supply chain provenance: transferring representations of device ownership

Device Manufacturer → Distributor → Consumer i → Consumer j
TXN A TXN B TXN C

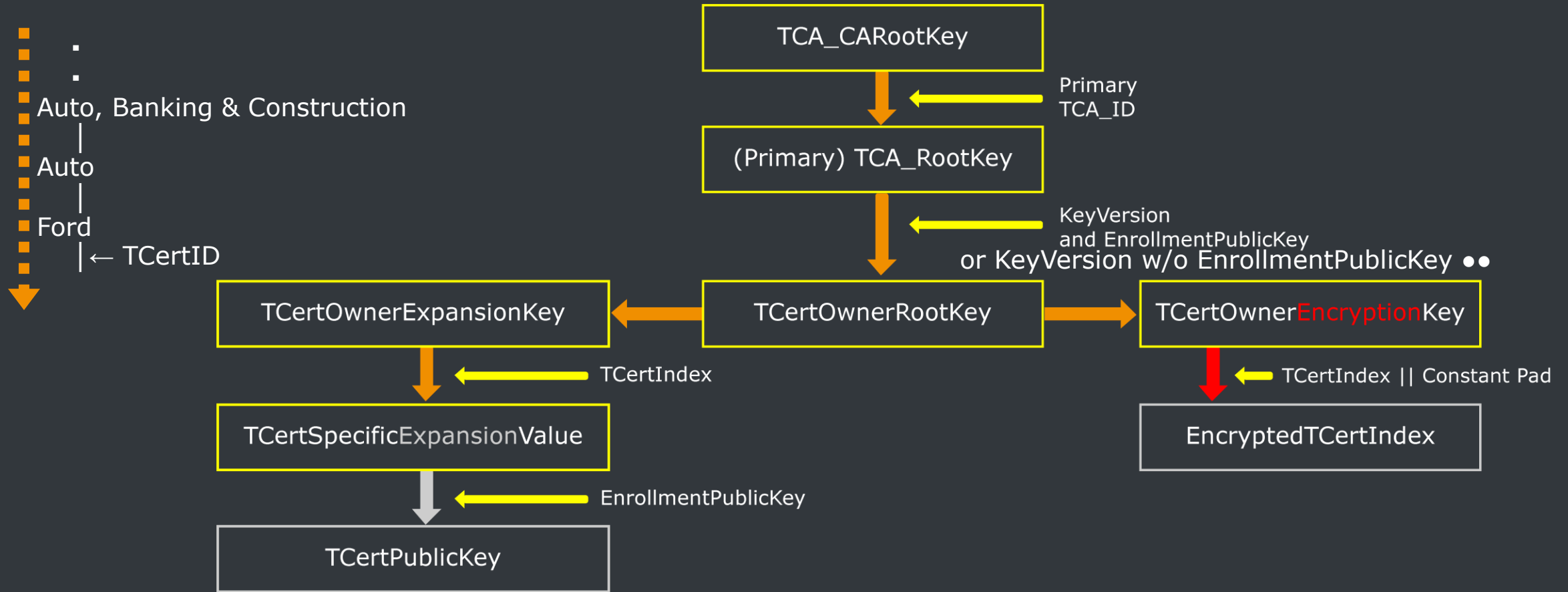


Device Creation (TXN A): payload \supset Device Serial Number(s); metadata \supset **Device Manufacturer signature TCert** with “selectively released” attribute(s) key(s) + **Device Manufacturer-acquired Distributor- owned key agreement TCert** with Distributor attribute key

First Sale (TXN B): payload \supset specific Device Serial Number and decryption key for payload of TXN A; metadata \supset **Distributor signature TCert** with attribute(s) key(s) + **Distributor-acquired Consumer i- owned key agreement TCert** with pseudonym attribute key

eBay (TXN C): payload \supset decryption key for payload of TXN B; metadata \supset **Consumer i signature TCert with pseudonym attribute key** (with pseudonym matching TXN B) + **Consumer i- acquired Consumer j- owned key agreement TCert with pseudonym attribute key**

Key Management



Thank you: Questions?

David.Kravitz@darkmatter.ae