SAND2015-8642C

Exceptional service in the national interest

Sandia National Laboratories

Physically Unclonable Digital ID*

Peter S. Choi, Ph.D., CISSP, CSSLP

* This disclosure of this presentation is the subject of at least U.S. Patent Application 62175753, entitled “METHODS AND SYSTEMS FOR AUTHENTICATING IDENTITY,” filed June 15, 2015, and U.S. Patent Application 62237253, entitled “Systems and Methods for Communicating Data Utilizing Dynamic Encryption,” filed October 5, 2015.”

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

- Sandia National Laboratories
  - Operated and managed by Sandia Corporation which is a wholly owned subsidiary of Lockheed Martin Corporation
  - SNL is a contractor to DOE's National Nuclear Security Administration (NNSA)
  - Number of Employees locations
    - About 10,000 employees work at ABQ headquarter
    - About 1,500 employees in Livermore, California, a second principal lab
  - SNL is a Federally Funded Research and Development Center (FFRDC)
  - Delivers science and technology to resolve the nation's most challenging security issues
  - Partners with
    - academia,
    - industry, and
    - government

Sandia National Laboratories (Cont.)

- Cooperative Research and Development Agreement (CRADA)
  - Stevenson-Wydler Technology Innovation Act of 1980
  - Permits SNL to transfer
    - technologies,
    - processes,
    - R&D capabilities, and
    - technical know-how to the private sector
  - Funding source and collaboration
    - Funds-in
    - In-Kind
    - Intellectual Property (inventions, copyrights, codes, designs, and blueprints)
    - Information exchange (NDA)
  - http://www.sandia.gov/working_with_sandia/agreements/crada/_assets/documents/BrochureExternal-CRADA-SAND2014_18916M.pdf

PUF

Sandia National Laboratories

- Physically Unclonable Function (PUF)
  - Energy flow pattern, uniquely tied to randomness inherent in the physical systems
  - “Fingerprint” of physical object
  - PUF uses (challenge, response) pair as protected secrets
    - Challenge component of the PUF only exists when device is used
    - PUF responses are difficult to spoof, clone, or predict
  - PUF’s intrinsic properties can be used as:
    - Random number generators
    - Device authentication
    - Encryption
    - Etc.
  - IC Examples: uncontrolled variability of the microfabrication processes
    - Arbiter
    - Ring Oscillator
    - Static Random Access Memory (SRAM)

Why do we need Solution like PUF?

Sandia National Laboratories

- Slew of digitized identity thefts
  - Target (40 Million Accounts), Home Depot (56 Million Accounts), JPMorgan Chase (76 Million Accounts)
  - OPM (~ 21 million identities)
- Christian Lusardi, Poker Tournament at Borgata, Atlanta City
- Lock/Unlock using your phone (Kevo Smart Lock, Okidokeys, Lockitron)
- Jeep Cherokee Hacked (Wired Article)
  - Brakes, steering wheel, transmission, radio
- Cybersecurity Consultant- Chris Roberts, charged with tampering with and taking control of United Airlines aircraft
- IoT presents “clear and present danger” ➔ not just toasters and refrigerators

State of Identity Management

Sandia National Laboratories

- Reliance on virtualized/digitized static ID
  - Clonable, replicable static information
    - Passwords, biometrics, PIV Cards ➔ Once digitized, becomes vulnerable
    - Identity verification based on static information is flawed
      - SSN, Birth Date, Mother's maiden name
  - One hacker can take-over million's of identities, remotely
- More secure means more annoyance
  - Multiple authentication, not multi-factor authentication
  - Event-based authentication
- Tokenized, non-replicable dynamic digital ID
  - True, two factor authentication
  - Solves the problem-of-scale (paradigm shift from one-to-many vs one-to-one attack model)

Why isn't PUF utilized more?

Sandia National Laboratories

- PUF phenomena arises from nano-scale diversity
  - Current manufacturing process do not have the control at the nano-scale
  - Nano-scale physical phenomena, highly susceptible to output noise, requiring mathematical model for error-correction
  - PUF often requires storing database of challenge-response pairs (CRPs) corresponding to the PUF component
    - If the response matches the stored response, the lock opens
    - In this PUF model, if CRP can be used only once, eventually running out of CRPs
    - Manufacturer has the access to CRP database ➔ ID is permanent
- Susceptible to modeling and cloning attacks
  - Access to device, access to challenge, response pair (CRP) behaviors
  - Have access to PUF's "response" pair

Why isn't PUF used more? (Cont.)

Sandia National Laboratories

- For consistent PUF behavior (complex error-correction algorithm is needed)
  - Needs "purified" energy source (e.g., homogenous current, voltage or light source)
  - Needs consistent environmental conditions (e.g. temperature, pressure, humidity)
- Difficult to define collision space with scalable deployment
  - Billions of device and billions of unique CRPs
  - CRP behavior is usually very complex and difficult to pin-down
- PUFs are permanent, cannot be modified to fit human ID
  - Manufacturers have access to device ID
  - Confidentiality of CRP is "intrinsically" compromised
- Securing PUF CRPs from manufacturing to deployment can be challenging and expensive

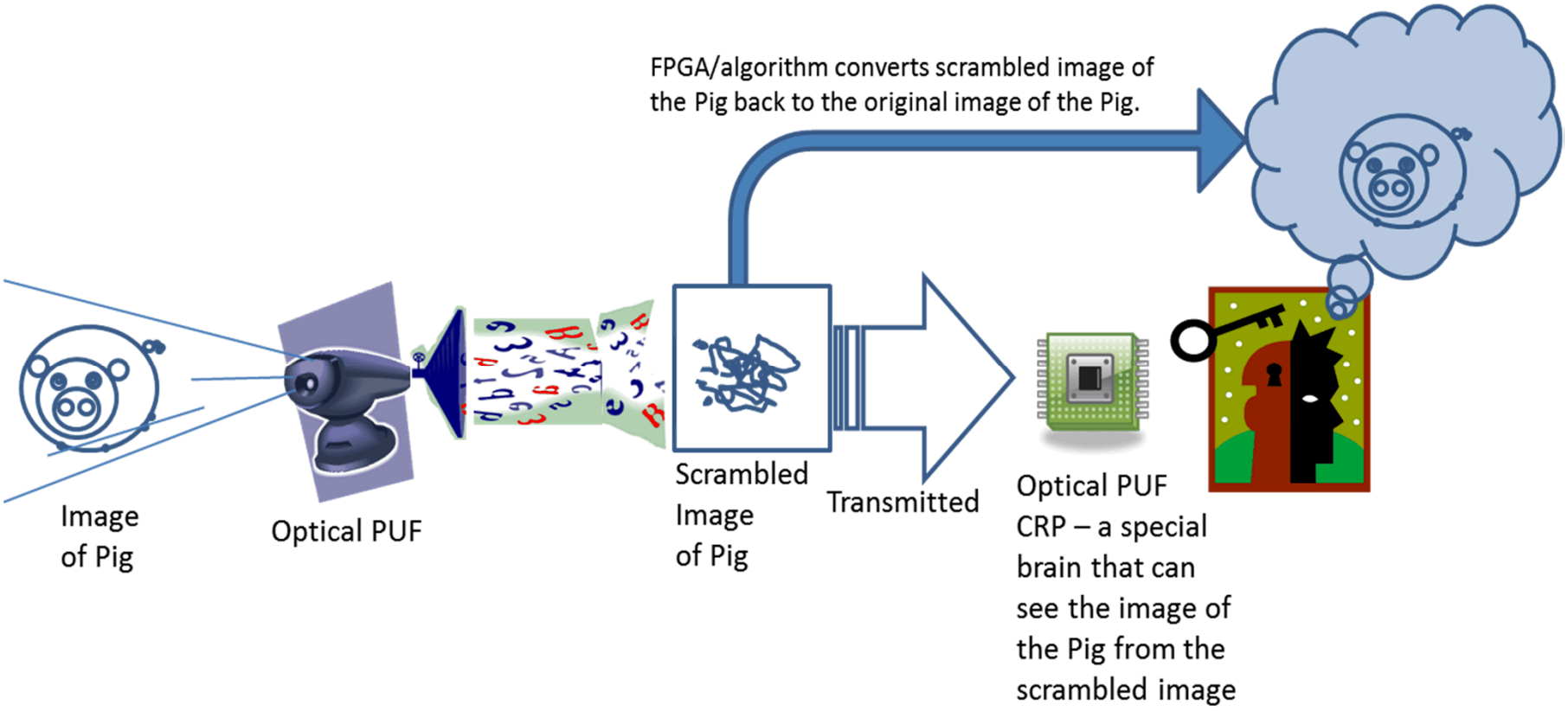
PUF Requires Complex Solution

If not PUF, then what? PUDID

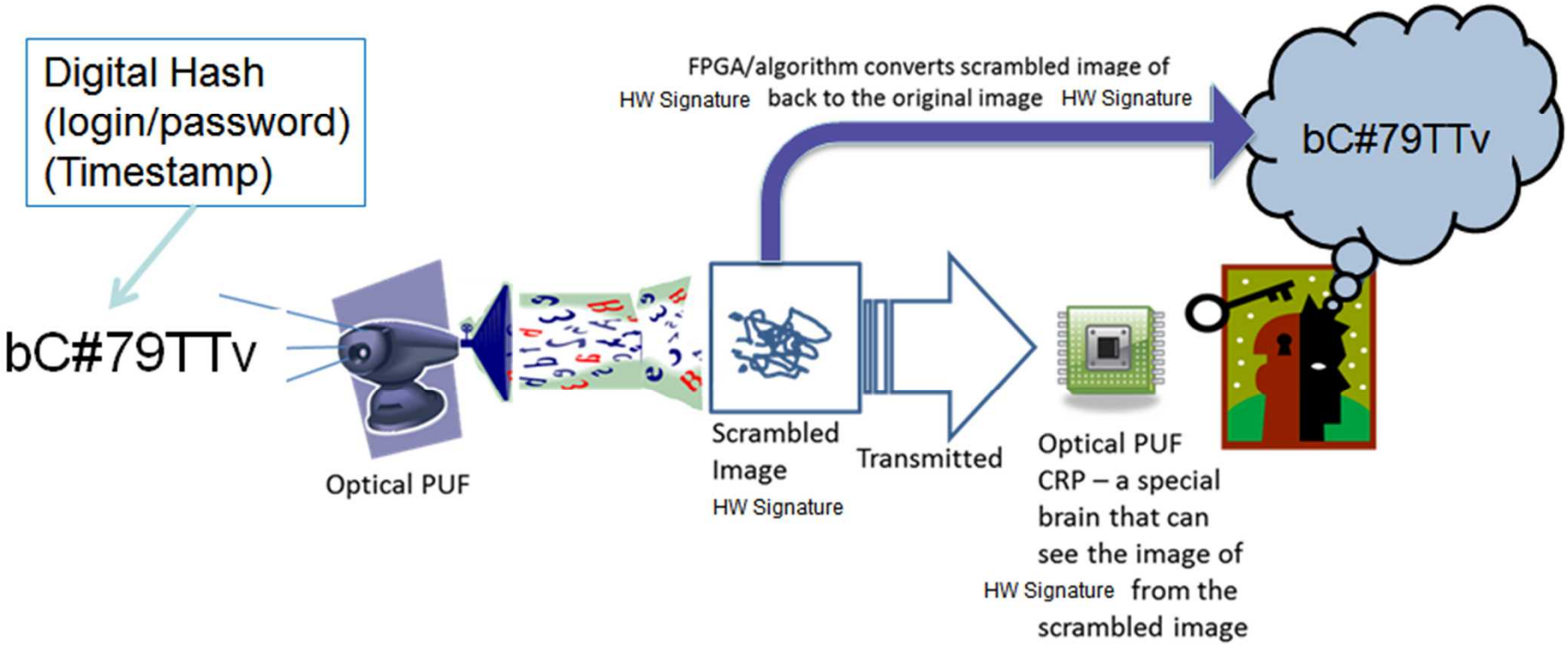
Sandia National Laboratories

- Time stamped digital hash “dynamic characters (DC)” is presented to sand blasted optical lens
- Recipient has the profile of possible “Responses” to CRP “Challenge”
  - Response profile can be released as “public key”
    - If there are billion devices, hackers must have billion CRP simulators
    - One directional identity verification (without dynamic “password hash”, PUF simulator is still useless)
  - Unclonable, physical “private key”

Macro-scale, Optics-Based PUF



Macro-scaled, Optics-Based Solution



Limitations of PUDID

Sandia National Laboratories

- PUFs are permanent, cannot be modified to fit human ID
  - Manufacturers have access to device ID
  - Confidentiality of CRP is “intrinsically” compromised
- Securing PUF CRPs from manufacturing to deployment can be challenging and expensive
- Another words, PUDID still have following limitations
  - Trusted Foundry Issue
  - No way to “create” verifiable human-machine coupled ID
- Can we come up with solution, non-PUF related but has the unique physical ID that can’t be copied while addressing above issues?
  - Quasi-Physically Unclonable Digital ID (Q-PUDID)

Quasi-Physically Unclonable Digital ID (Q-PUDID)

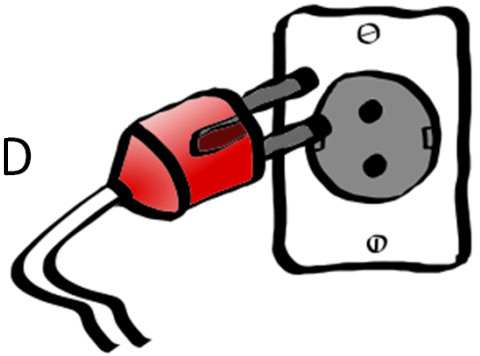
Sandia National Laboratories

- Process that integrates series of hashing algorithms and combining it with tamper resistant hardware functions to produce "unclonable, dynamic" digital ID
  - "unclonable": Near impossible or cost prohibitive to repeat
  - "dynamic": based on unique energy-material interaction behavior
- Uses macroscopic phenomena, instead of nanoscale phenomena

Innovation in Q-PUDID

Sandia National Laboratories

- Emulates PUF functionality
  - Macroscopic, physical phenomena ➔ Mathematically reproducible
  - Tamper resistant technology ➔ Unique, uncompromisable device ID
  - Discrete application of hash functions ➔ Dynamic ID
- Q-PUDID Authentication protocol
  - Extremely "protocol light"
  - Cheap to produce, hard to replicate
  - Pluggable and modular
- Authentication based on novel, unclonable digital ID
  - Does not use Confidentiality (e.g., encryption)
  - Enables "true" two form factor authentication
  - ID is non-static
  - Digital ID is grounded in physical world
  - Integrates seamlessly to exiting "login/password" legacy system



integration simplicity

Q-PUDID

- Cyber identity, anchored to unique physical device, intentionally made very hard to replicate (e.g., tamper resistant)
- No possibility of a mass breach (tokenized authentication on steroid)
  - Criminals must steal your device and your credential (password/biometrics) ➔ 2 Factor Authentication
  - Identity is verified through dynamic, non-static authentication that must process through your physical key

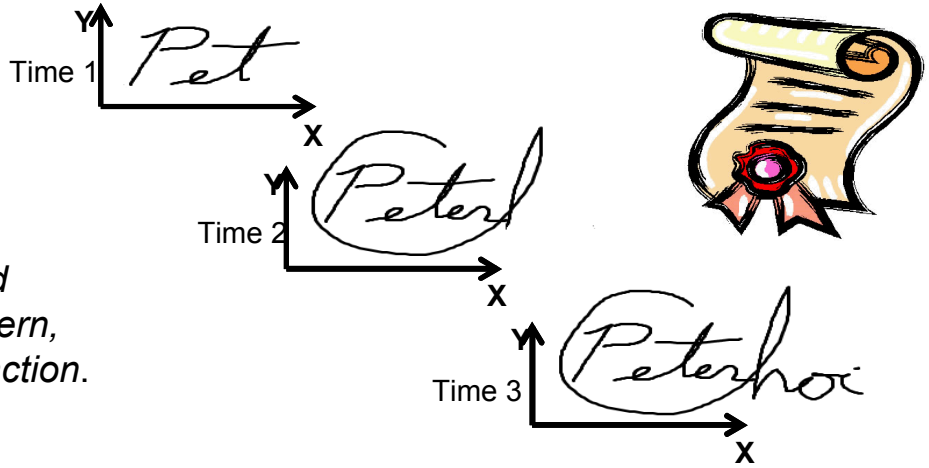
Q-PUDID

- Q-PUDID is scalable
  - More secure but less cumbersome
  - Identity collision probability, mathematically scaled according to needs ➔ Hole in one shot is still hole in one shot irrespective of how many people achieve it.
- Current PIIs no longer needs to be kept confidential

Quasi-PUDID Device: Activation

Example of Quasi-PUF Device

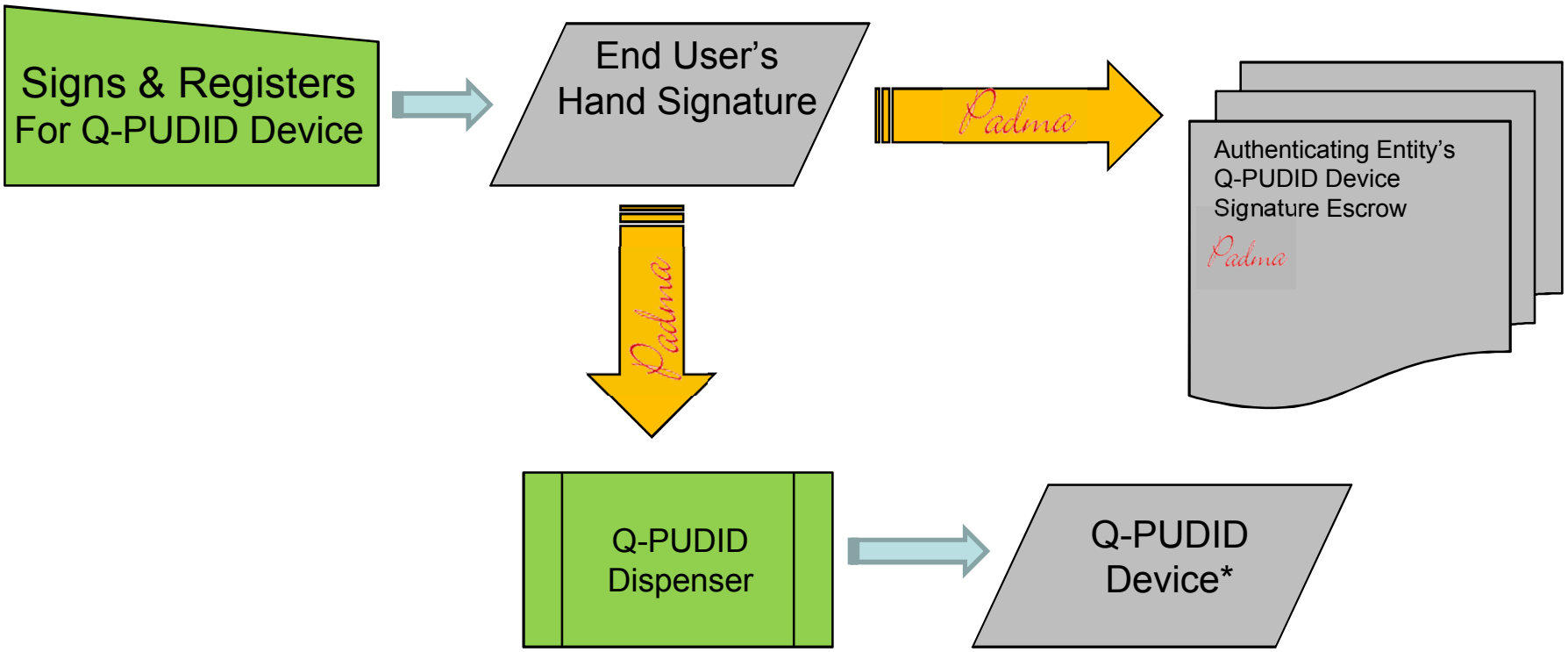
- Random pattern is burned into Q-PUDID device
  - For bank application, assume time sensitive hand signature is tied to human ID



Unrepeatable, one-time hand signature is captured and used as unique physical device pattern, "burned" into the black box function.

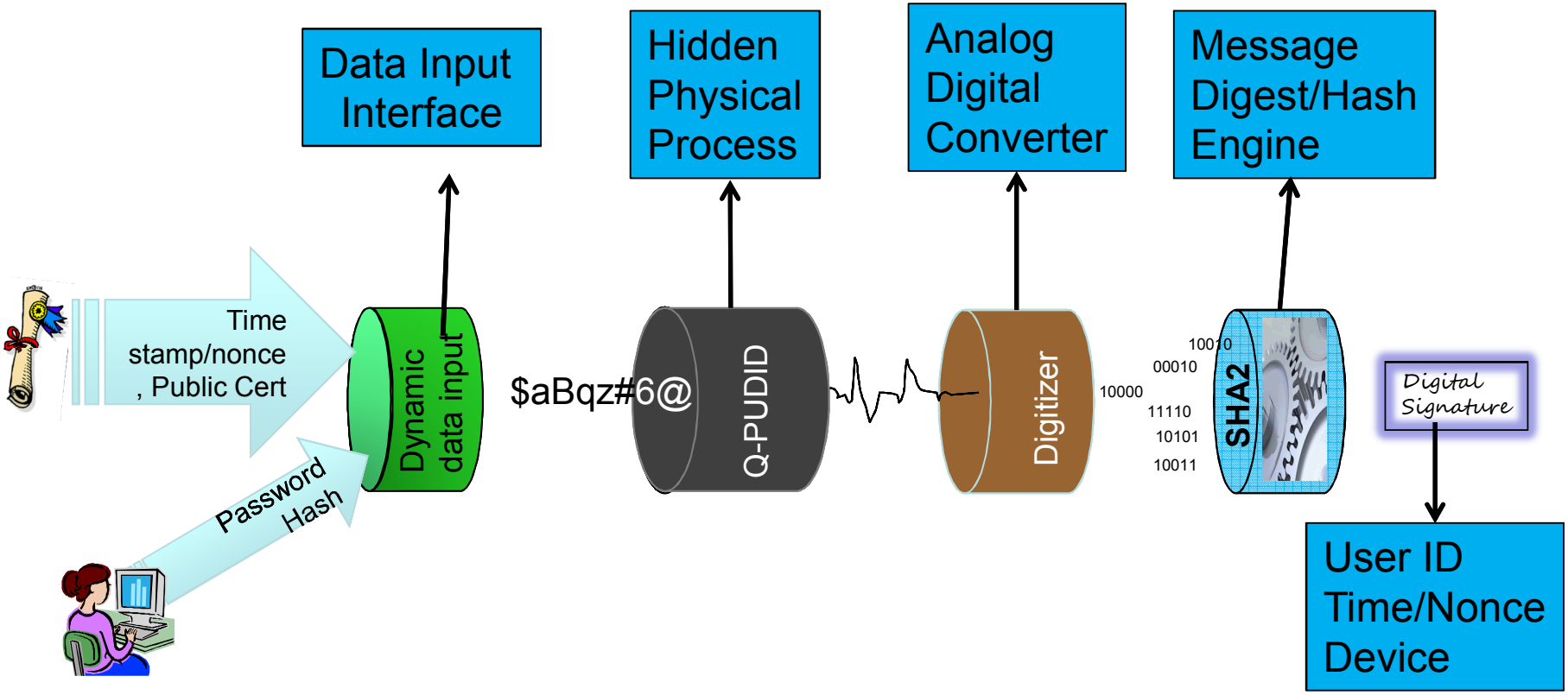
- This "random pattern" is physically stored under tamper resistant hardware such as Smart Card chip
- This "random pattern" is designed to interact with in-flow of data and modifies the data unique to this "random pattern"
- This modified data is put through message digest function producing digital signature validating the person's ID and the Q-PUDID hardware

Quasi-PUDID Device Activation Process



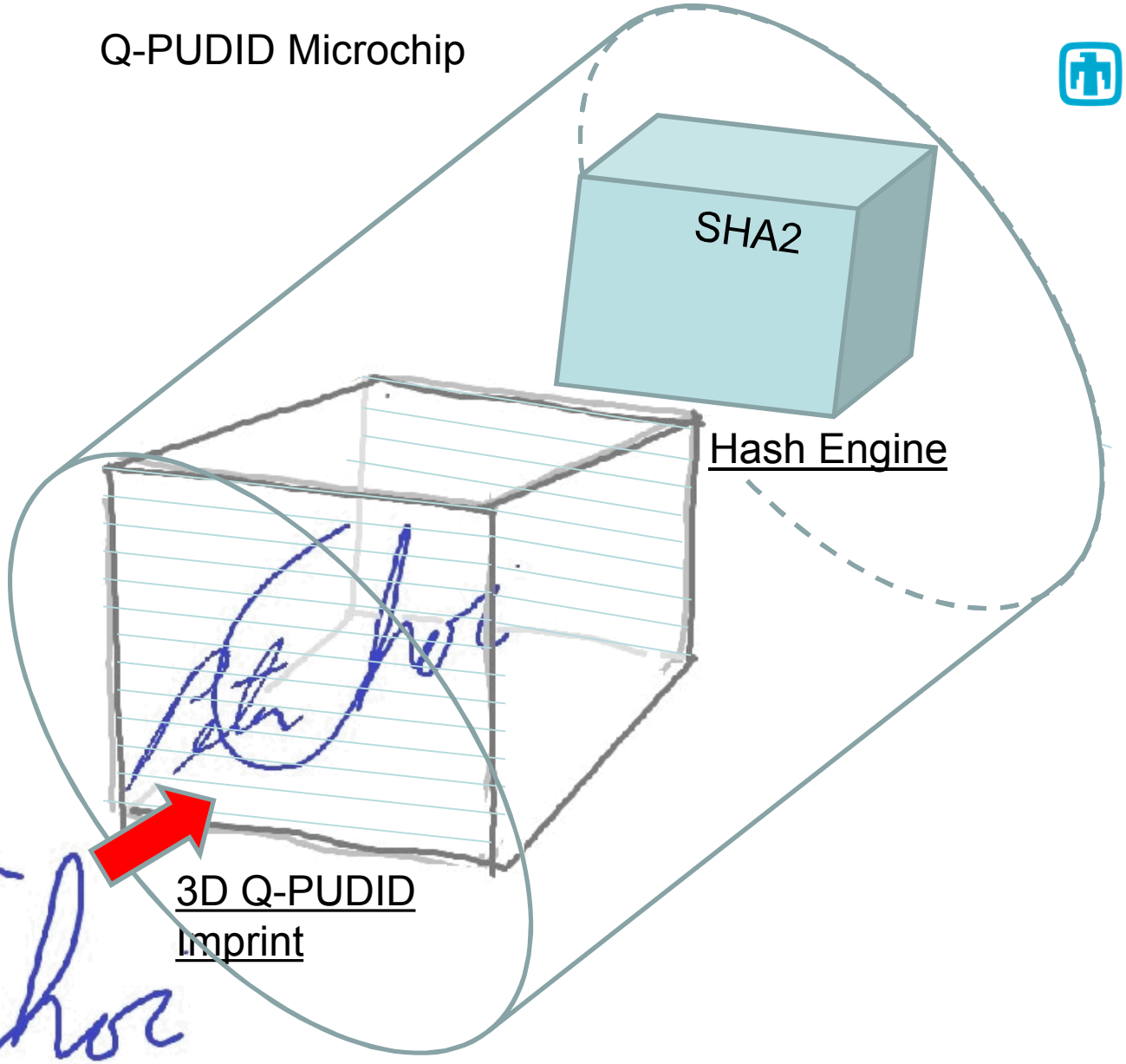
* End user's signature is burned into Q-PUDID device and by design, it is never read by any external inquiries

Quasi-PUDID Device



Q-PUDID Microchip

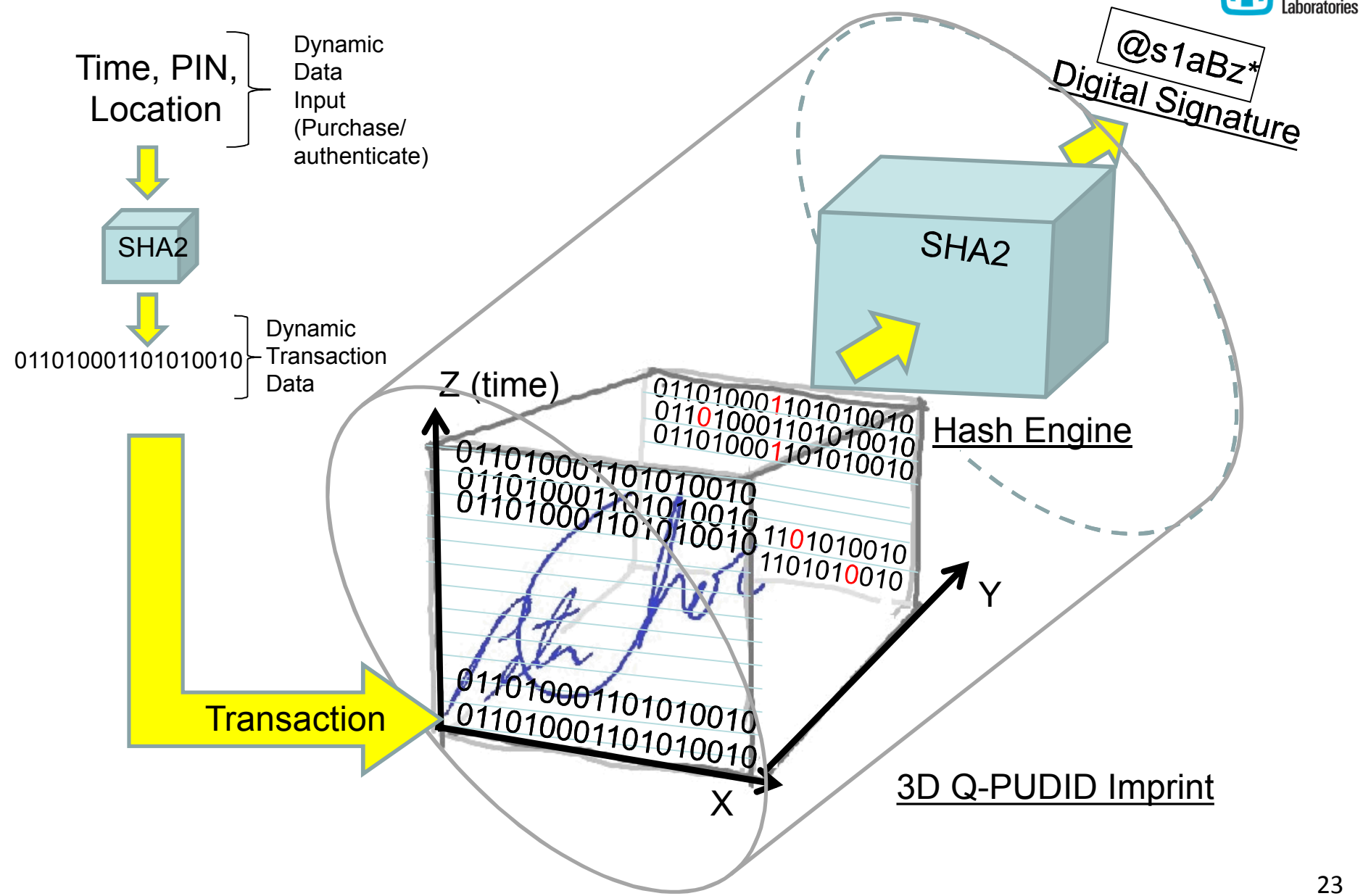
Sandia National Laboratories



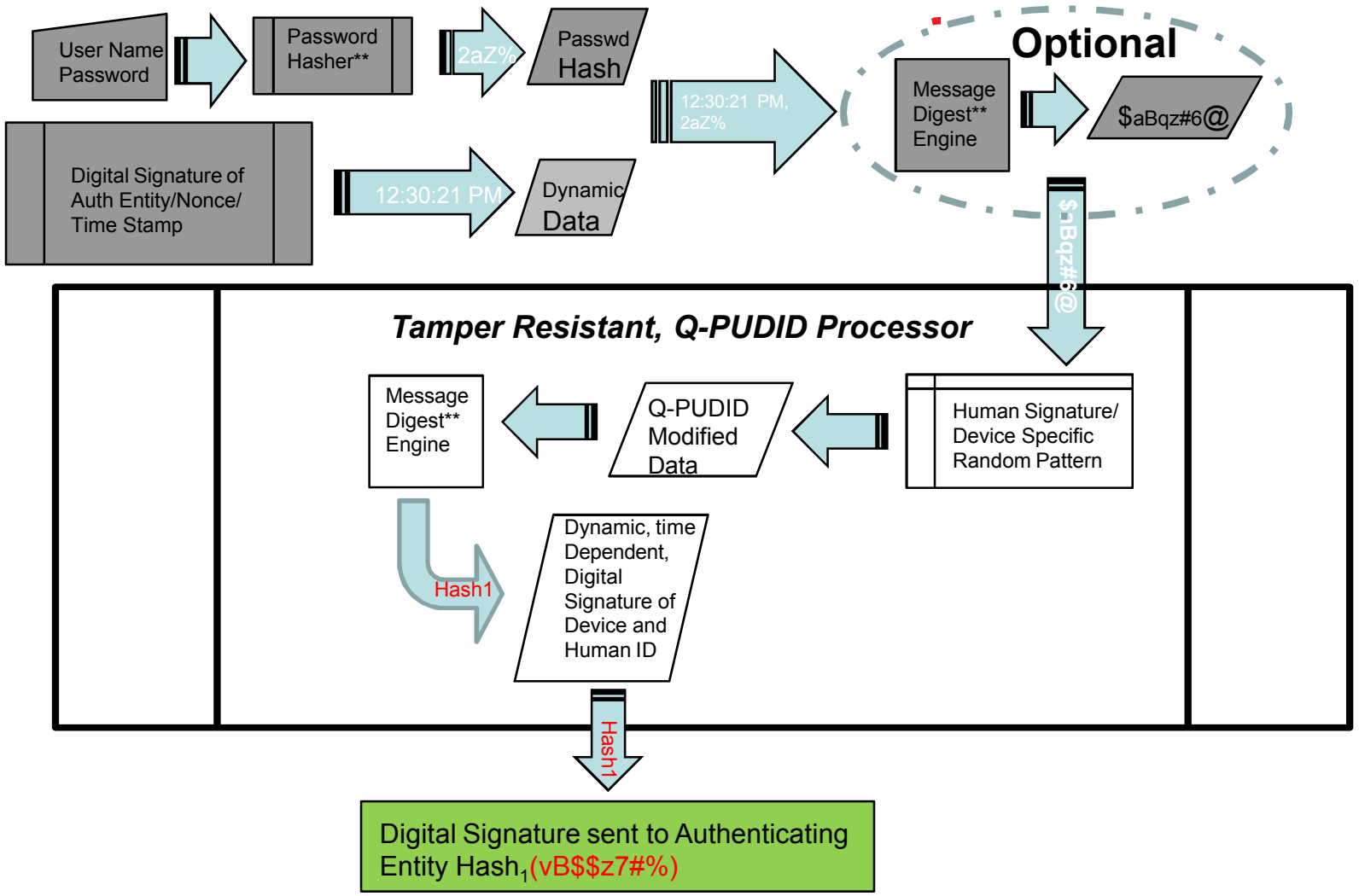
Q-PUDID Registration

Hand Signature

Q-PUDID Transaction



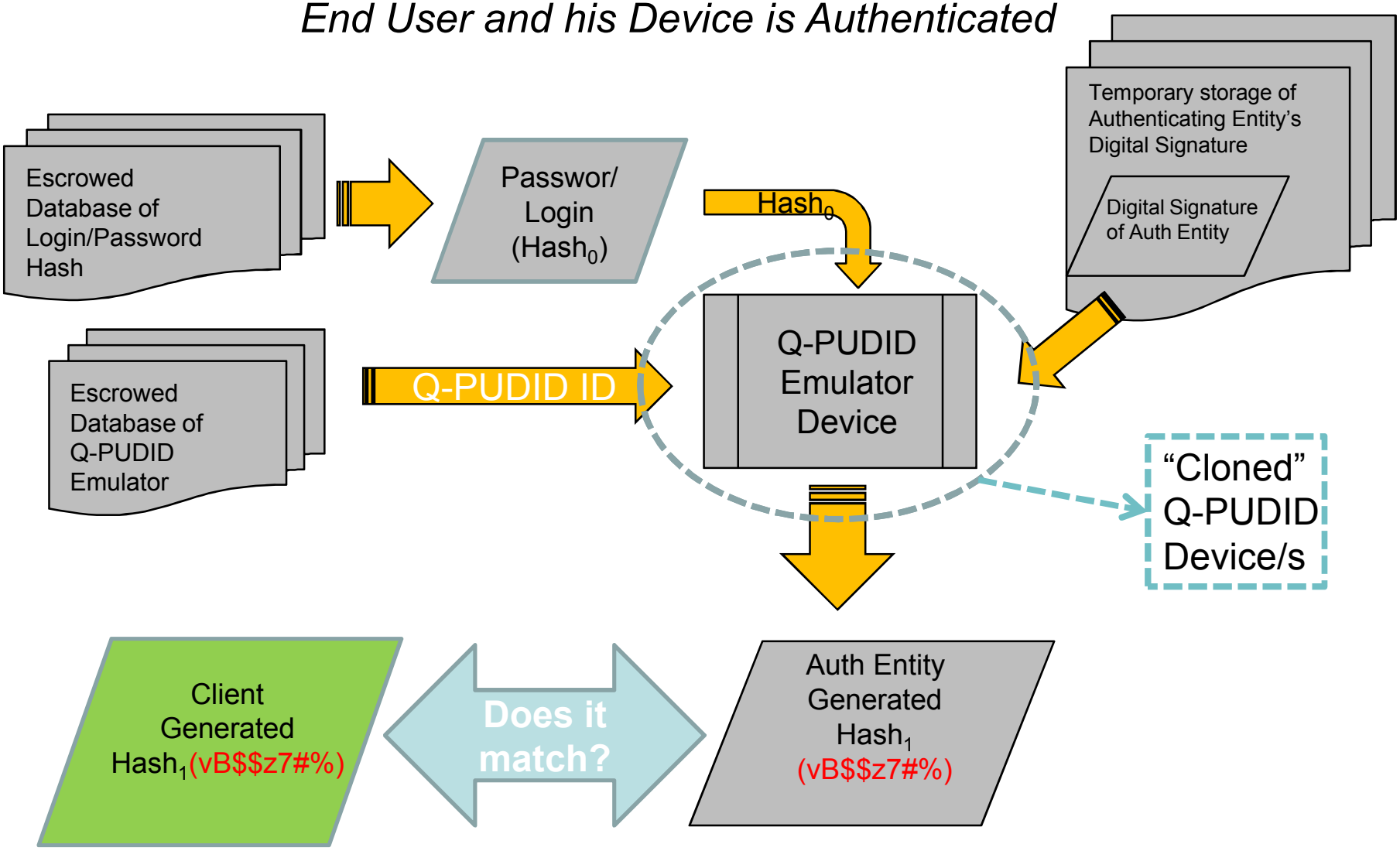
Q-PUDID Device (Digital)



**Message Digest and Hash functions are used inter-changeably

Q-PUDID Application: Authenticating Entity

End User and his Device is Authenticated



Key Features of Q-PUDID

Sandia National Laboratories

Standard Authentication	Q-PUDID Authentication
Uses password or PIN to access “static data” on the secure chip	Passwords/PIN are just used as dynamic input to creating physical signature of a secured chip
Confidentiality/Encryption is used to “securely transmit” digital ID	Integrity (Hash function) is used to authenticate device and human ID
Digital ID can be replicated and processed by any generic computing device	Digital ID can only be validated by being processed through unique Q-PUDID device
Remote identity theft is rampant & completely possible (1 to many model)	Access to physical Q-PUDID device is necessary to compromise Q-PUDID identity (1 to 1 model)
Stronger authentication usually means greater inconvenience to end-users	Q-PUDID is extremely convenient, near impossible to spoof remotely
New multi-factor authentication requires having completely different infrastructure	Q-PUDID is a plug-in solution that integrates into existing legacy infrastructure

Potential Q-PUDID Application

Sandia National Laboratories

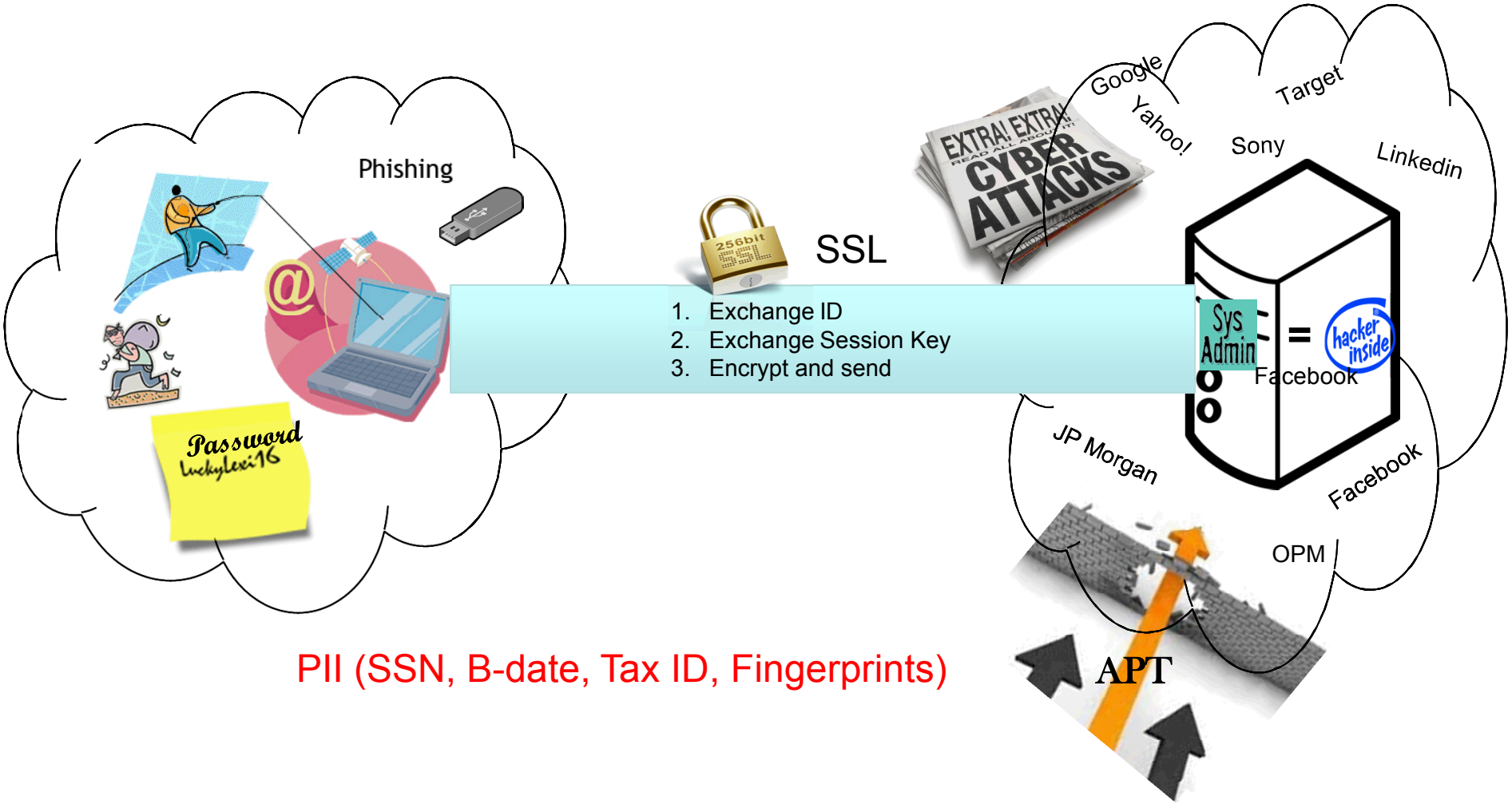
Q-PUDID Applications:

- IoT Authentication (machines that can uniquely identify other machines)
  - Electronic Control Unit (ECU for auto-industry)
  - Multi-factor, Unclonable Access Control Card
  - Secure drone management
  - Smart/Secure Meter
  - Multi-media control (cable set top box)
  - Secure casino chips
  - Prevent digital take-over of passenger airplanes
  - Etc.
- Human-Machine Authentication
  - Security cameras and sensors
  - Computing devices and IT resources
  - Point of Sale (POS) system
  - Mobile ATM
  - Authentication for wearable technologies (Smart Watch, iPhones)
  - Gaming console(s)
  - Etc.

Current State of Cyber Security

Sandia National Laboratories

>75% all Hacks, Compromise
in Digital Identities



PII (SSN, B-date, Tax ID, Fingerprints)

SSL/TLS Process

Sandia National Laboratories

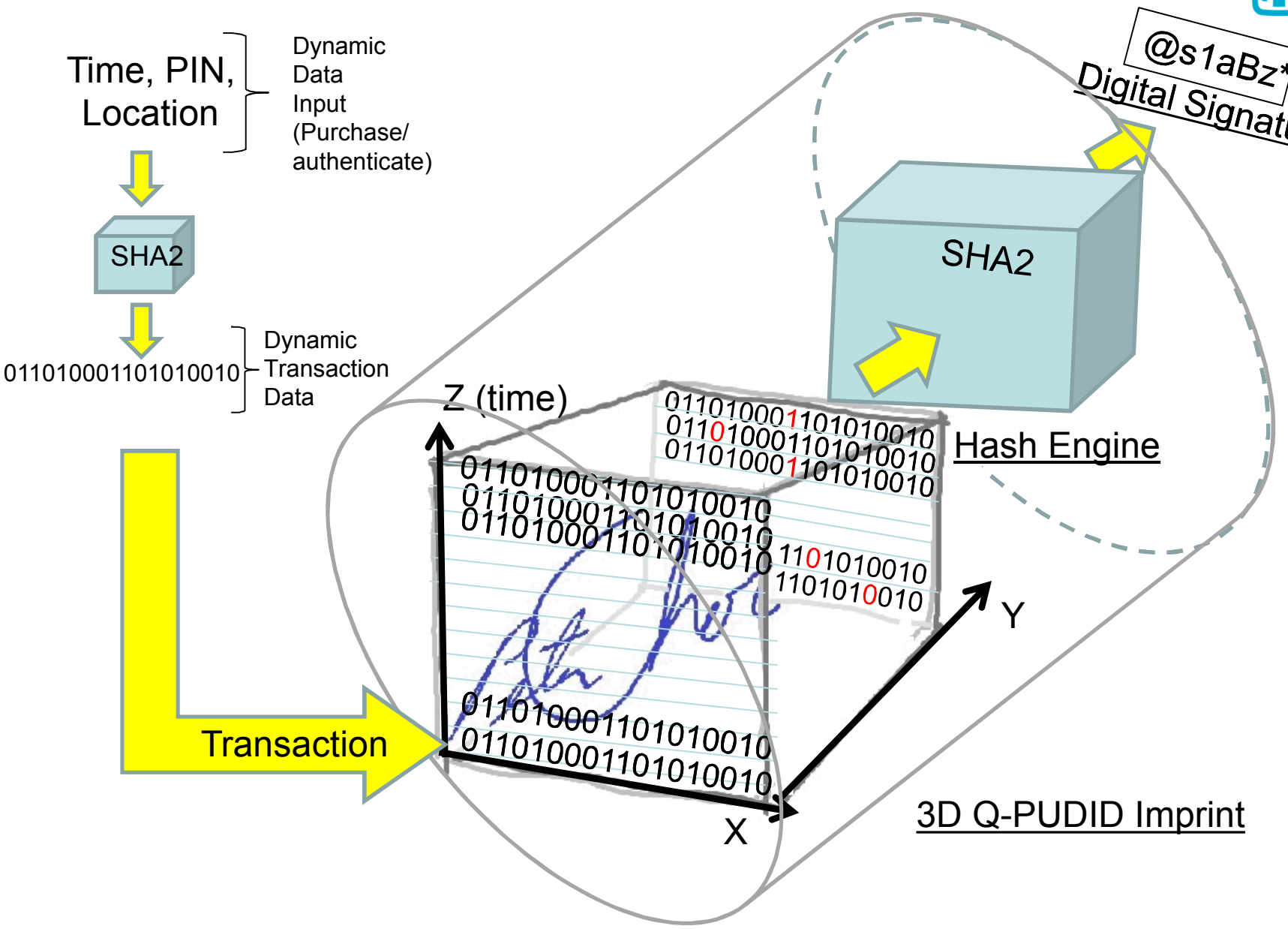
- SSL/TLS Process Description
  1. Private Key is stored on the client and server side
  2. Identities are exchanged and validated via PKI
  3. A session encryption key is generated and exchanged between server and client
  4. Data is encrypted, usually be client, and sent to server
  5. Server decrypts the data
- SSL/TLS Issues
  1. SSL/TLS built on asymmetric algorithm (RSA, DH, ECC)
  2. SSL/TLS susceptible to quantum computing development (Shor's algorithm)
  3. NSA's Information Assurance Directorate
     - Initiated transition to quantum resistant algorithms
     - https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

Dynamic Packet Encryption Protocol

Sandia National Laboratories

1. Client uses Q-PUDID signature as “seed” to dynamically generating encryption key for each packet
2. Encrypted packet is sent along with clear text of user ID and time
3. Receiving end, server, uses “user ID and time” to generate the packet encryption key to decrypt the packet
4. Every packet will have unique encryption key

Q-PUDID Transaction



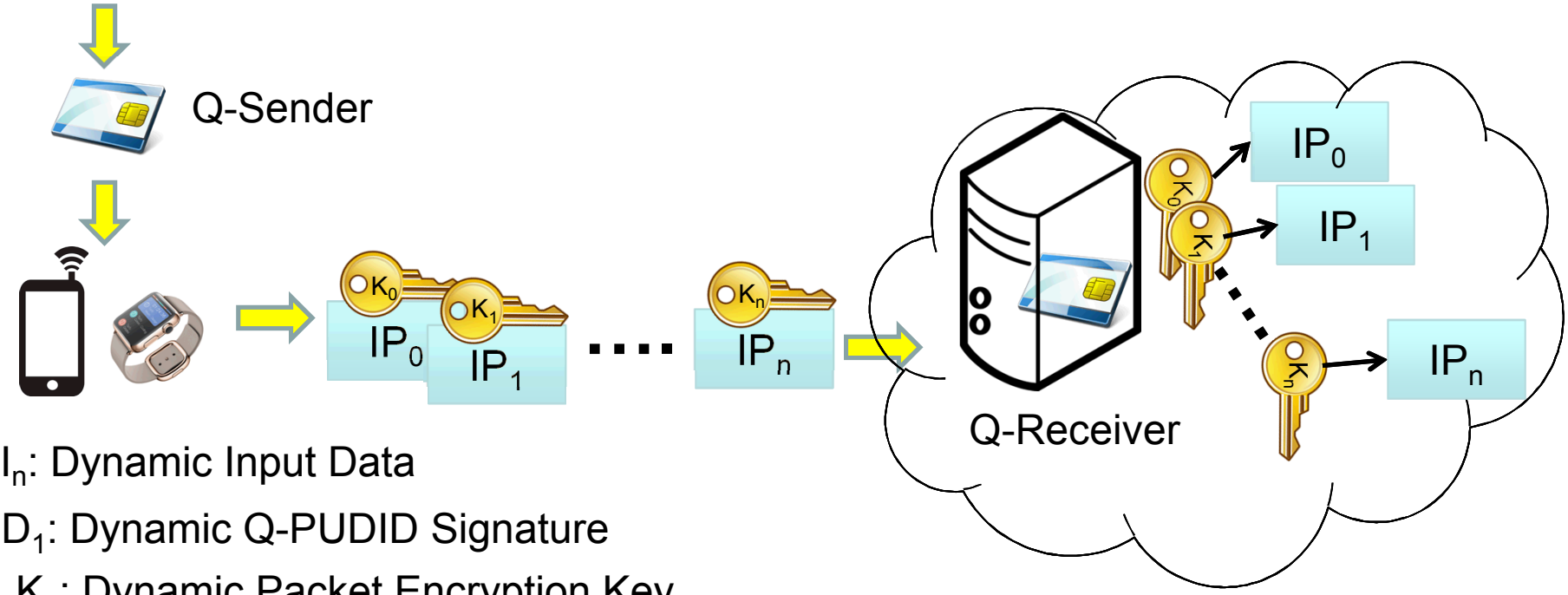
Dynamic Packet Encryption Protocol

Sandia National Laboratories

$I_0(Time_0, PIN, Location_0) = I_0 \rightarrow$ Q-PUDID $\rightarrow D_0 \rightarrow K_0$

$I_1(Time_1, PIN, Location_1) = I_1 \rightarrow$ Q-PUDID $\rightarrow D_1 \rightarrow K_1$

$I_n(Time_n, PIN, Location_n) = I_n \rightarrow$ Q-PUDID $\rightarrow D_n \rightarrow K_n$



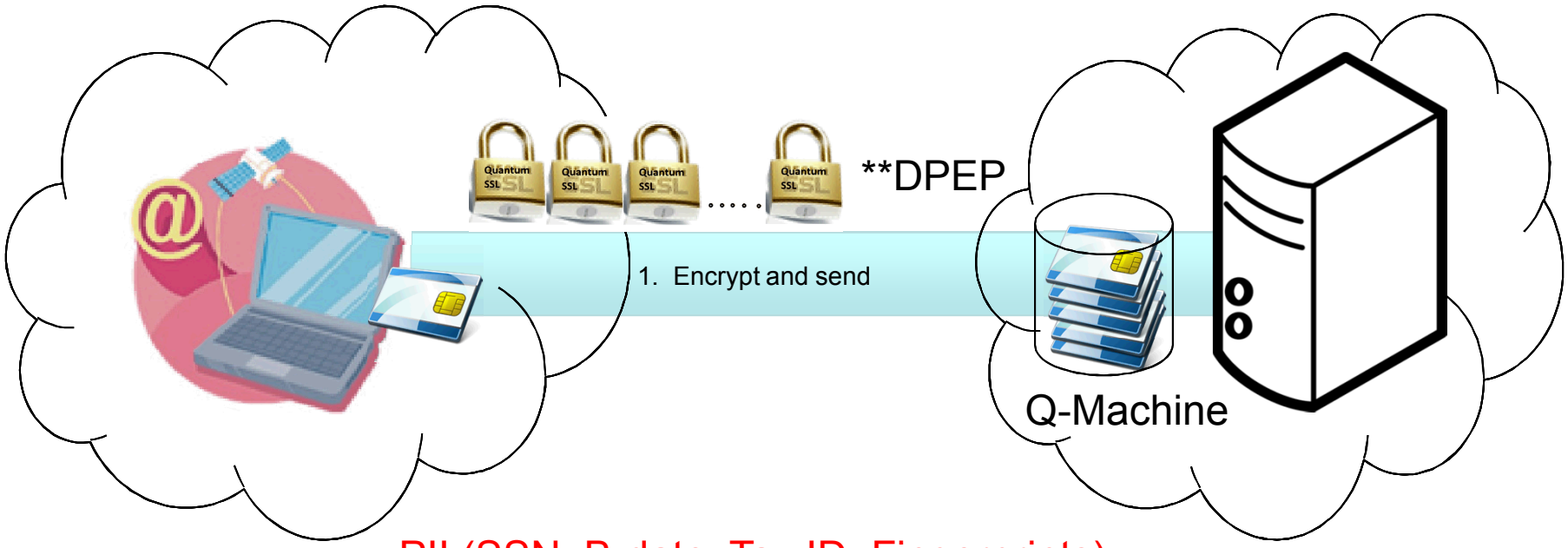
I_n: Dynamic Input Data

D_1: Dynamic Q-PUDID Signature

K_n: Dynamic Packet Encryption Key

IP_n: IP packets

Physically Unclonable Digital ID



PII (SSN, B-date, Tax ID, Fingerprints)

Becomes Public Data

PII(SSN, B-date, Tax ID, Fingerprints)

**DPEP: Dynamic Packet Encryption Protocol

CRADA Status

- Provisional Patent Filed: June 15, 2015
- Quantum resistant SSL, Provisional Patent Filed
- FBO Announced:
  - June 26, 2015…will be closing on September 26, 2016
  - https://www.fbo.gov/spg/DOE/SNL/SN/15_440/listing.html
  - Asking for funds-in
  - Multiple CRADAs possible
- News coverage
  - http://www.iotjournal.com/articles/view?13327/3
  - https://govtribe.com/person/schoi-at-sandia-gov/activity
- Interested Companies (Multiple CRADAs possible)

Conclusion

- Q-PUDID protocol is foundational - many new applications are possible
  - Extremely protocol light
  - Identity verification is impervious to MitM or Replay attacks
- Sandia partnership offers:
  - Potential access to existing patent rights
  - Working model/demo of Q-PUDID application
  - Opportunities to co-own additional patents surrounding Q-PUDID application(s)
  - Available Sandia resources
    - Subject matter experts (SMEs)
      - Nuclear, biological, computational, MEMS labs, etc.
      - Red-teaming capabilities, independent security validation
- Sandia's reputation
  - Serving the needs of National and International security
  - DOE, DoD, DHS, other government agencies
  - Connection to World class universities and other National Labs

Sandia National Laboratories

Questions?

Dr. Peter S. Choi
schoi@sandia.gov

Active Drone Management

Sandia National Laboratories

- Unmanned Aerial Vehicles
  - Rising military and private industry use
  - Protect against Threat actors
    - Seal the critical information drones contain
    - Crash, sabotage or commandeer the drone in flight
    - Tack-over scenario
    - RF-enabled cyber attacks have been demonstrated
- Q-PUDID application to drone management
  - Preconfigured Cognitive Command & Control (P3C)
    - Mutual active authentication between ground station (GS) and UAVs
    - Every command from GS is actively authenticated
    - Q-PUDID, an exploit-resistant authentication and C&C

Smart Meter

Sandia National Laboratories

- Miniature computing device that measures the consumption of utilities and communicates back to service provider via
  - Wireless mesh network
  - Power line networking
  - Connection to the user's own Internet service
- Unmanned, unmonitored utility device
  - Lack of authentication service ➔ IoT authentication problem
  - Lack of data integrity and confidentiality ➔privacy, data tampering
- Susceptible to remote cyber attacks
  - Meter tampering
  - Man-in-the-middle
  - Invasion of privacy
- Q-PUDID Implementation
  - Replace human "what you know" factor with meter GPS location data and time