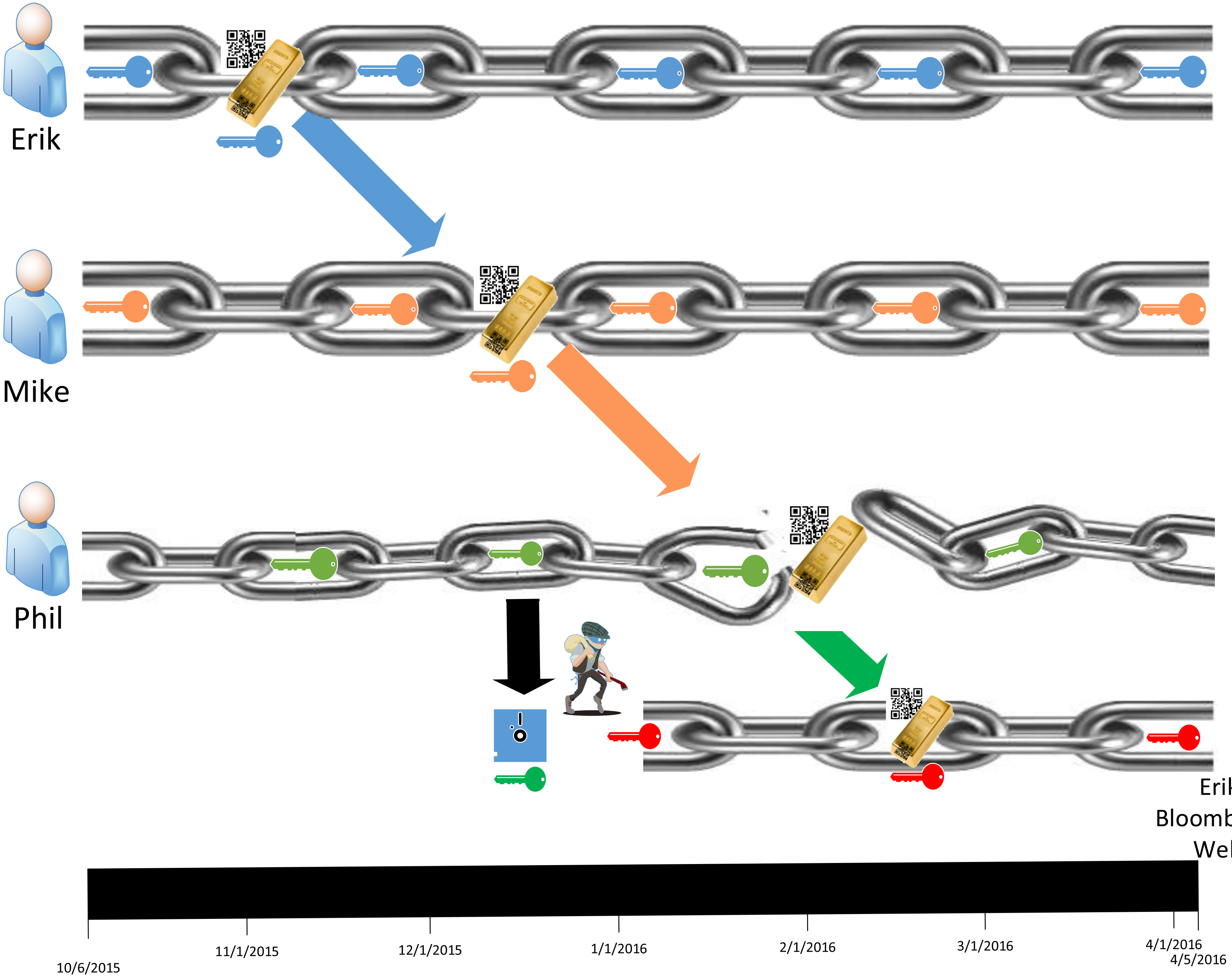
Identity theft is easier with current Blockchain. Its just 1 private key and the protected assets are yours.

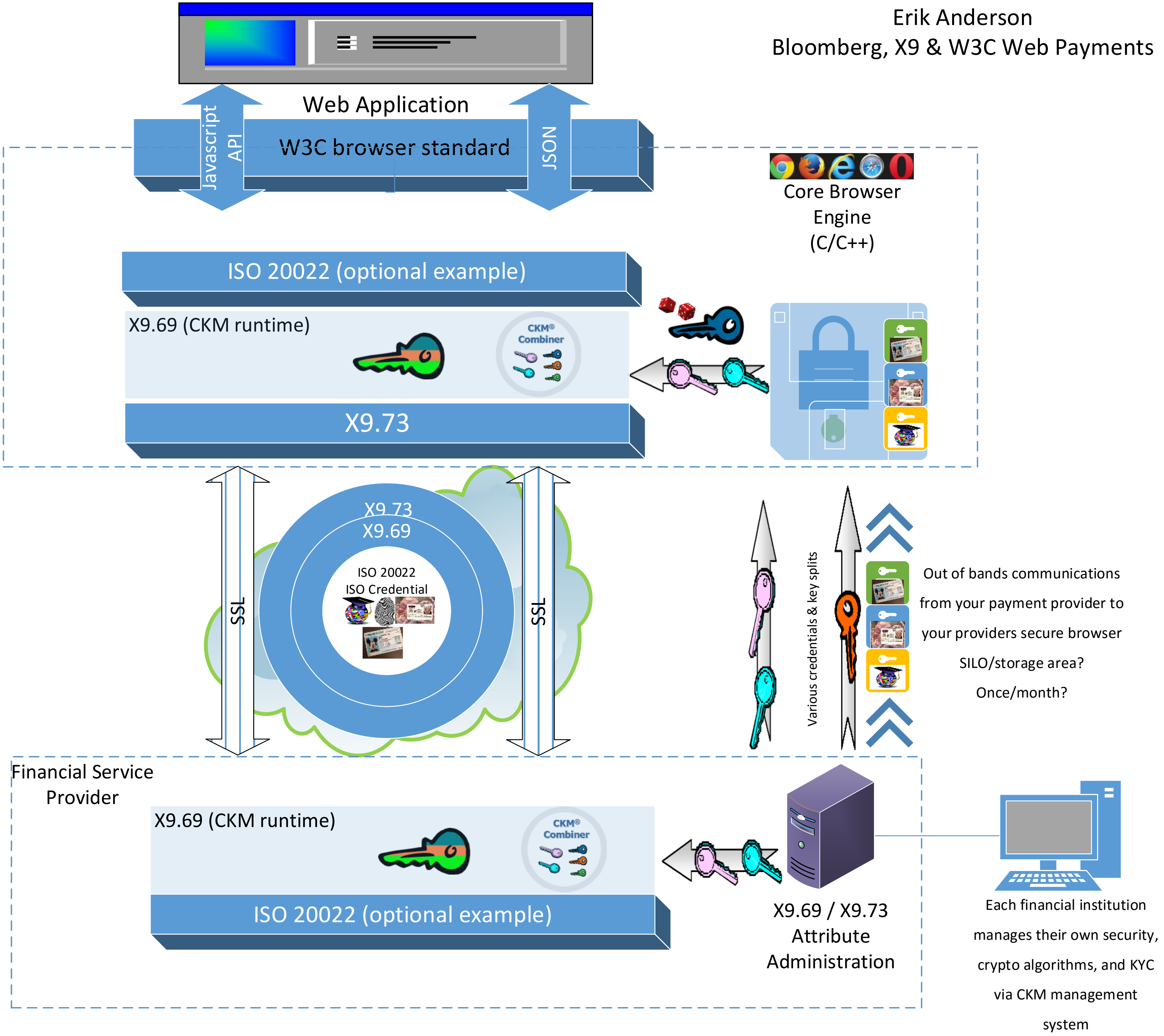
Public: 1BoJiyRnCN5E2FEG3gbC85d6h3c7Xmcqs1

Private: 5KgEvEvubwVJGjVBr8UZPe73kksTLk2dqVXh3JavzGaaJSQBUk4



Erik Anderson
Bloomberg, X9 & W3C
Web Payments

Erik Anderson
Bloomberg, X9 & W3C Web Payments



Web Application

Javascript API

W3C browser standard

JSON

Core Browser Engine (C/C++)

ISO 20022 (optional example)

X9.69 (CKM runtime)

X9.73

SSL

X9.73

X9.69

ISO 20022

ISO Credential

Various credentials & key splits

Out of bands communications from your payment provider to your providers secure browser SILO/storage area? Once/month?

Financial Service Provider

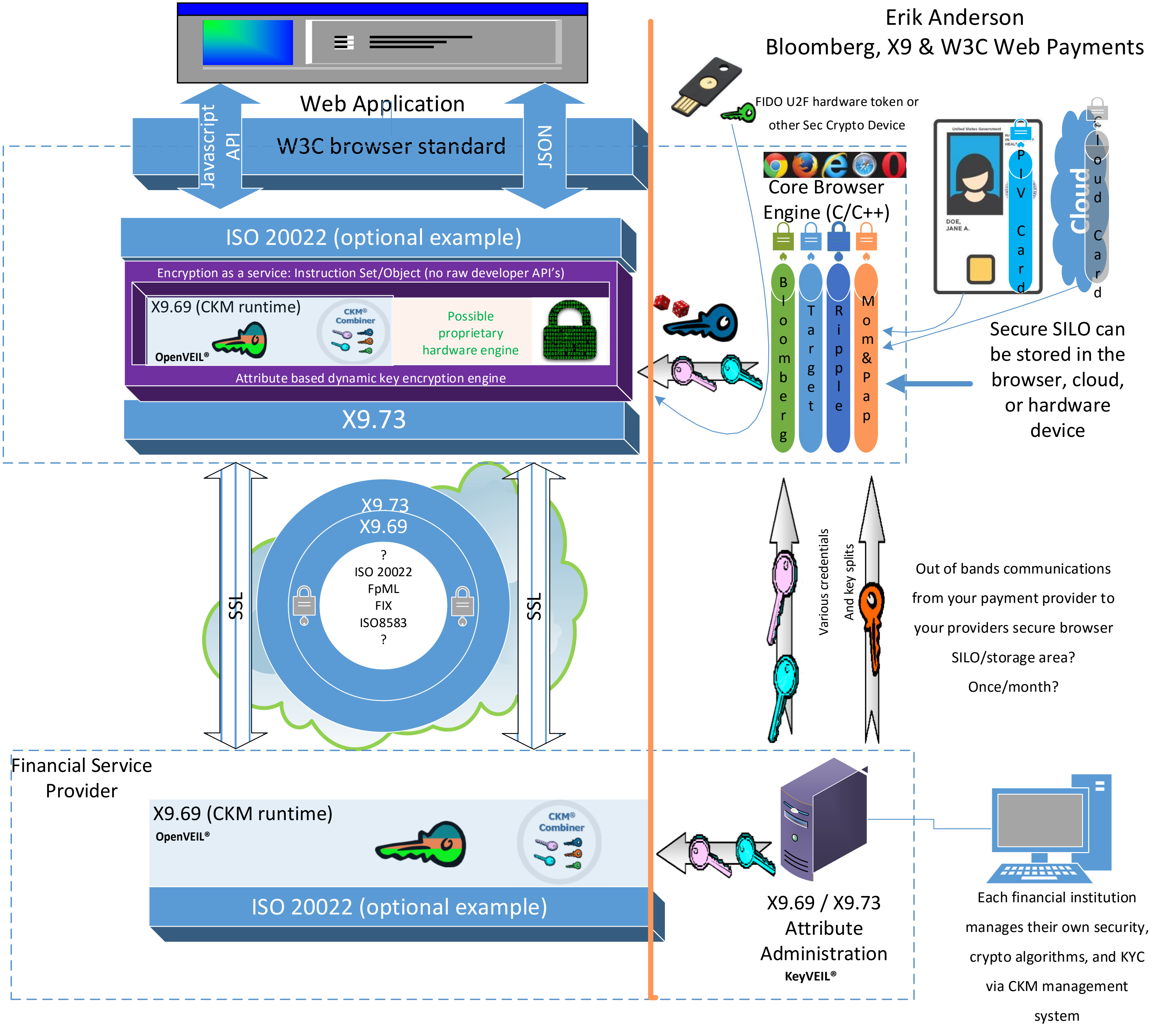
X9.69 (CKM runtime)

ISO 20022 (optional example)

X9.69 / X9.73 Attribute Administration

Each financial institution manages their own security, crypto algorithms, and KYC via CKM management system

Erik Anderson
Bloomberg, X9 & W3C Web Payments

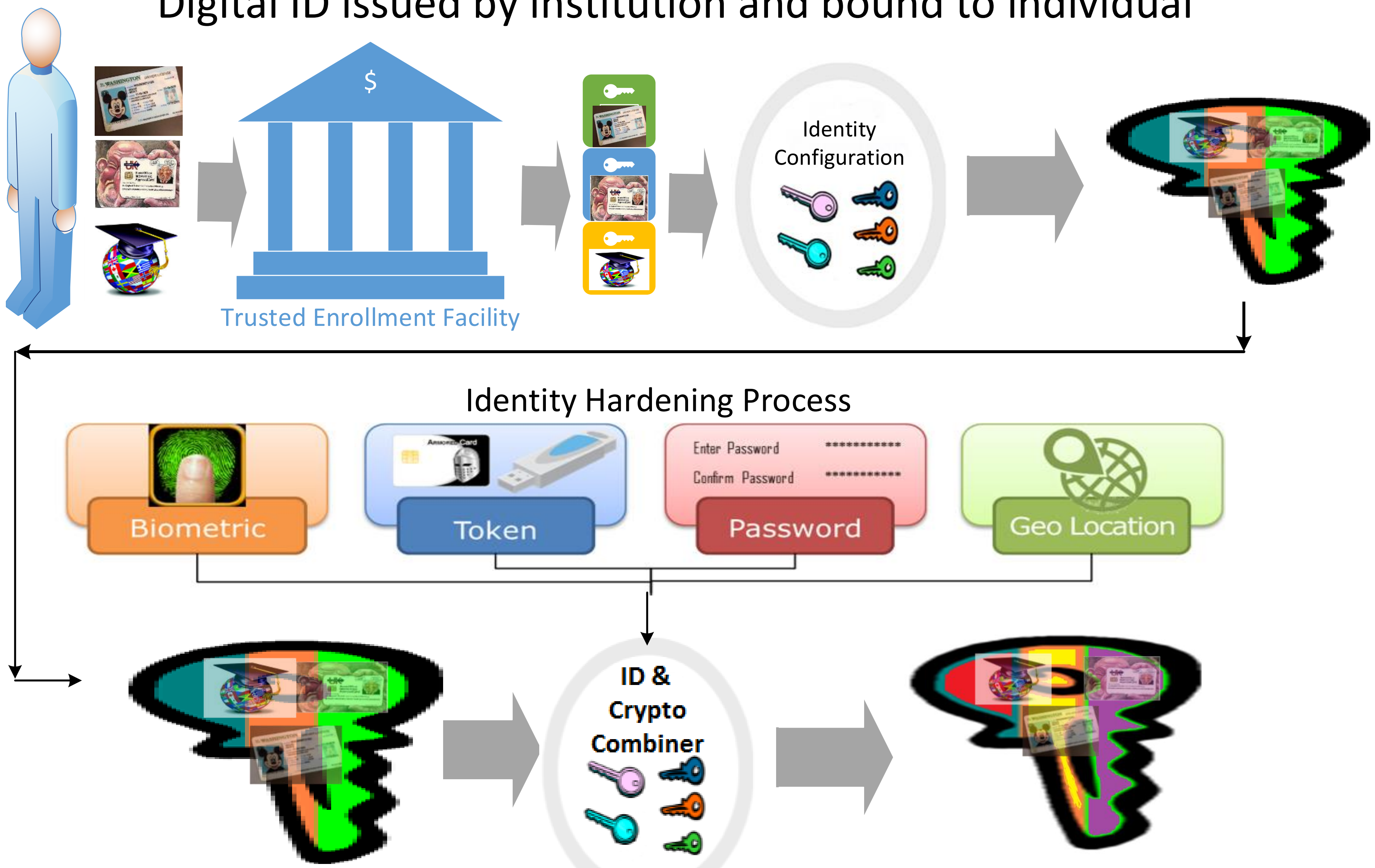

Web Application
Javascript API
W3C browser standard
JSON
ISO 20022 (optional example)
Encryption as a service: Instruction Set/Object (no raw developer API's)
X9.69 (CKM runtime)
OpenVEIL®
CKM® Combiner
Possible proprietary hardware engine
Attribute based dynamic key encryption engine
X9.73
SSL
X9.73
X9.69
?
ISO 20022
FpML
FIX
ISO8583
?
SSL
Financial Service Provider
X9.69 (CKM runtime)
OpenVEIL®
CKM® Combiner
ISO 20022 (optional example)
FIDO U2F hardware token or other Sec Crypto Device
Core Browser Engine (C/C++)
Bloomberg
Target
Ripple
Mom&Pap
PIV Card
Cloud
Cloud Card
United States Government
DOE, JANE A.
Various credentials
And key splits
X9.69 / X9.73 Attribute Administration
KeyVEIL®

Secure SILO can be stored in the browser, cloud, or hardware device

Out of bands communications from your payment provider to your providers secure browser SILO/storage area? Once/month?

Each financial institution manages their own security, crypto algorithms, and KYC via CKM management system

Identity Based Encryption
or
Digital ID issued by institution and bound to individual



Trusted Enrollment Facility

Identity Configuration

Identity Hardening Process

Biometric

Token

Password

Geo Location

ID & Crypto Combiner

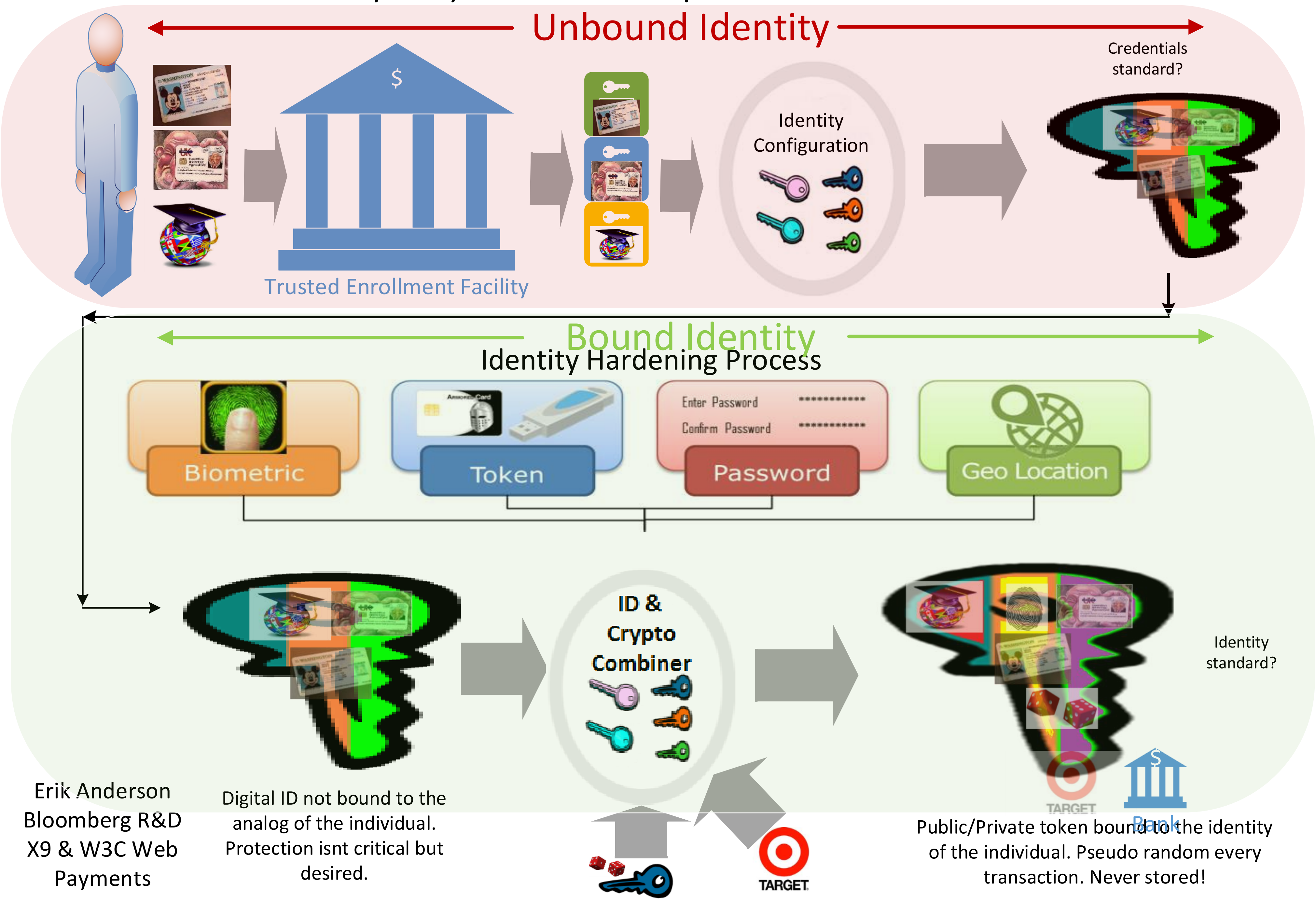
Erik Anderson
Bloomberg R&D
X9 & W3C Web Payments

Digital ID not bound to the analog of the individual. Protection isnt critical but desired.

Public/Private token bound to the identity of the individual. Private is never stored only created.

Privacy Respecting Identity Management

Random Identity every transaction with permissioned mathematical forensics



Unbound Identity

Trusted Enrollment Facility

Identity Configuration

Credentials standard?

Bound Identity

Identity Hardening Process

Biometric

Token

Password

Geo Location

ID & Crypto Combiner

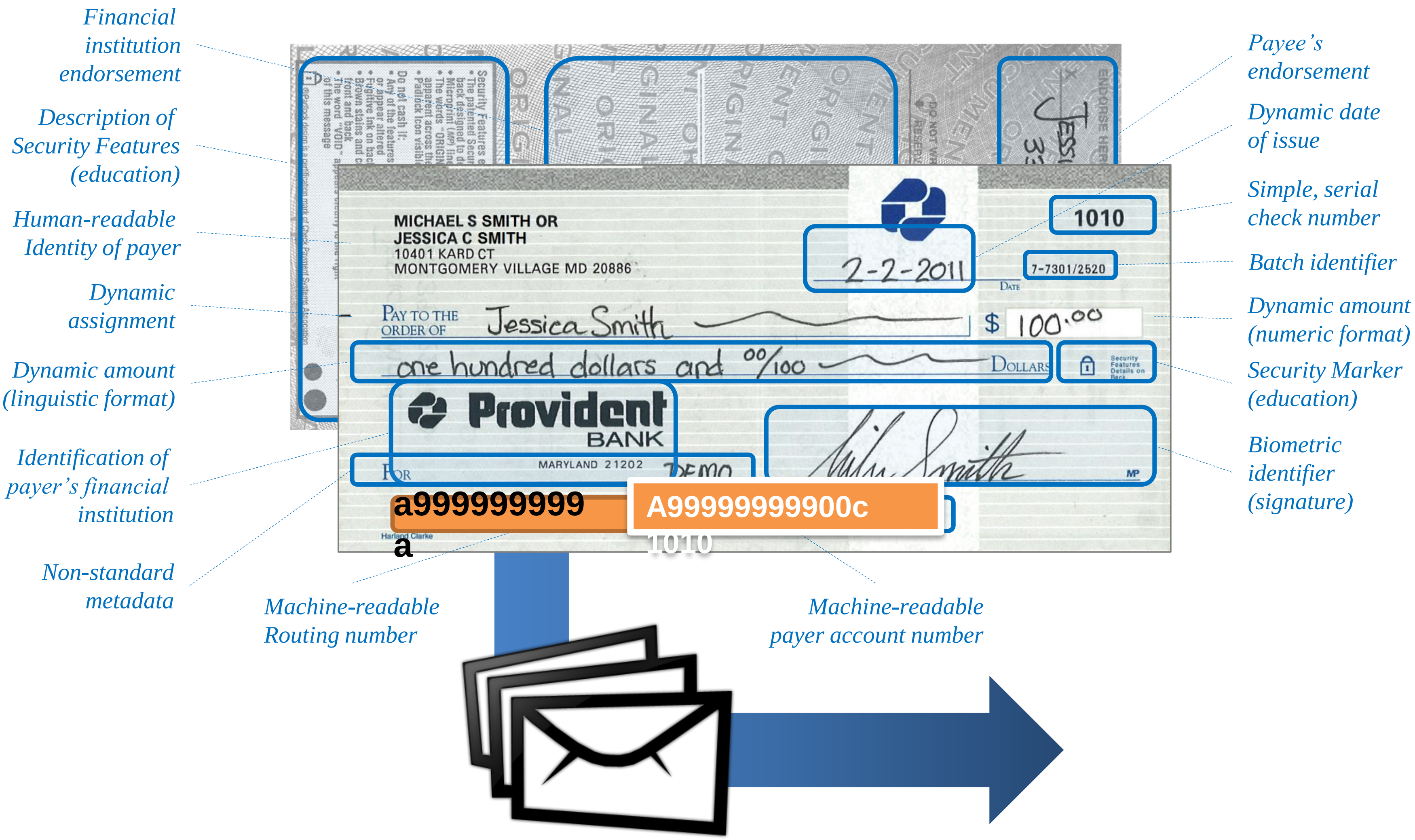
Identity standard?

Erik Anderson
Bloomberg R&D
X9 & W3C Web Payments

Digital ID not bound to the analog of the individual. Protection isnt critical but desired.

Public/Private token bound to the identity of the individual. Pseudo random every transaction. Never stored!

So, What is a Self-Contained Data Object?



MICHAEL S SMITH OR
JESSICA C SMITH
10401 KARD CT
MONTGOMERY VILLAGE MD 20886

1010

7-7301/2520

2-2-2011 DATE

PAY TO THE ORDER OF Jessica Smith $ 100.00

one hundred dollars and 00/100 DOLLARS

Provident BANK
MARYLAND 21202

FOR DEMO

a999999999a A99999999900c 1010

Financial institution endorsement

Description of Security Features (education)

Human-readable Identity of payer

Dynamic assignment

Dynamic amount (linguistic format)

Identification of payer's financial institution

Non-standard metadata

Machine-readable Routing number

Machine-readable payer account number

Payee's endorsement

Dynamic date of issue

Simple, serial check number

Batch identifier

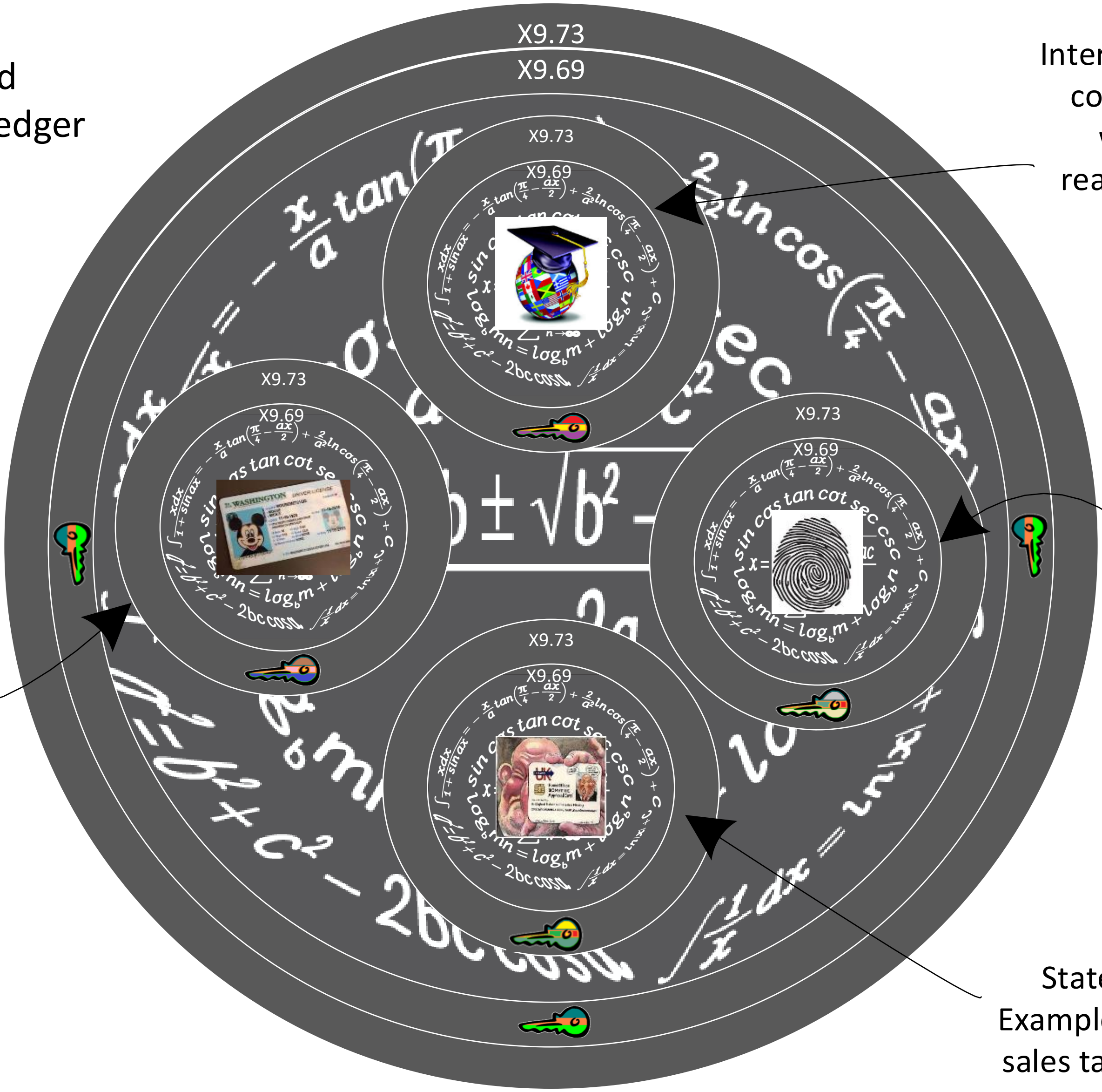
Dynamic amount (numeric format)

Security Marker (education)

Biometric identifier (signature)

Identity, like a passport, is assigned globally but permissions are local. Requires cryptographic objects with varying levels of permissions for each data & identity element. Each tier of regulators could get access to the individual elements they are authorized to see (not an inch more)

Example: One record written to a public ledger or Blockchain



International regulatory and compliance Information written for and only readable by International Regulatory bodies

Biometrics and Identity based encryption to bind the digital goods to me whether the goods are on my hard drive, cloud, or even a Blockchain

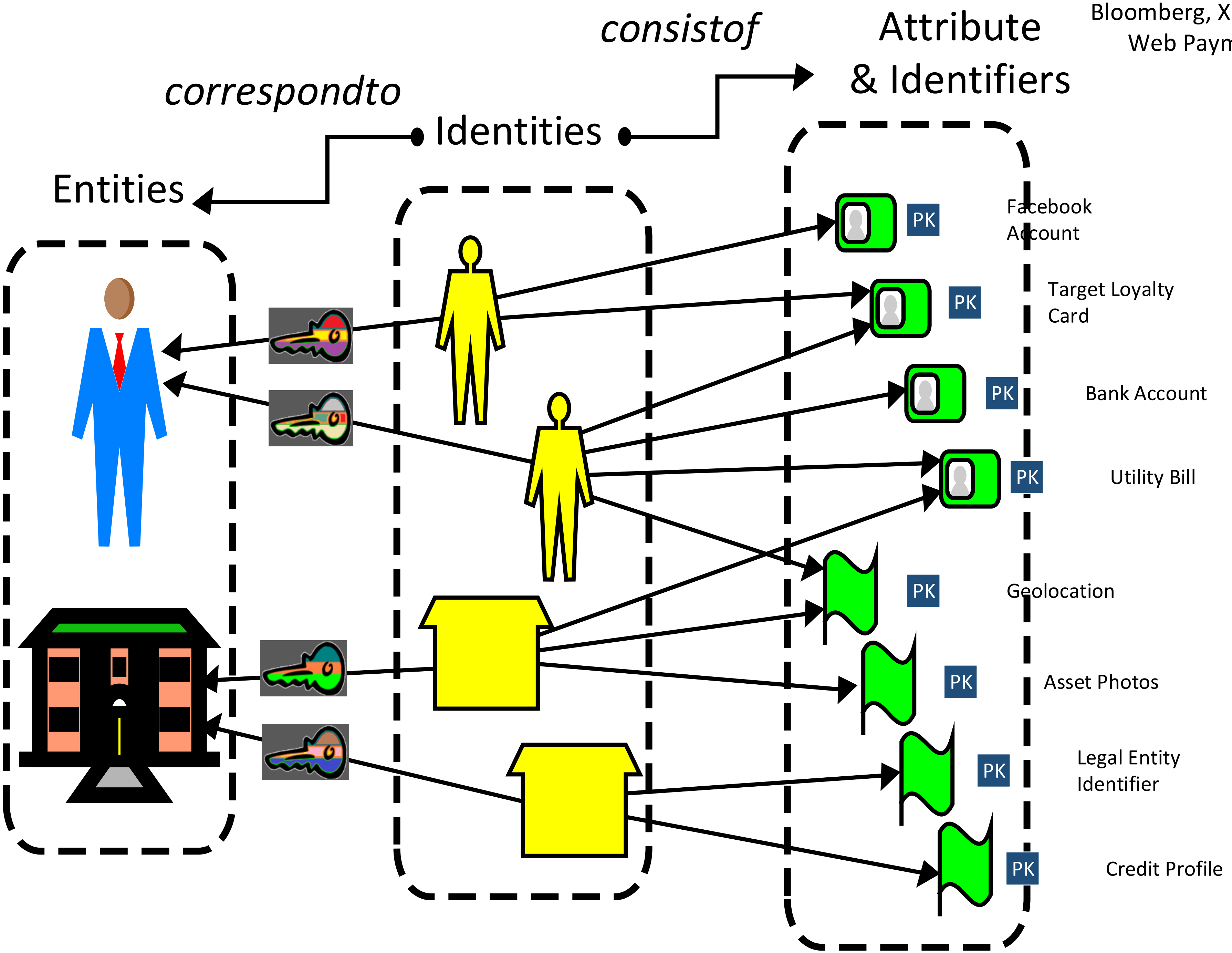
Transaction value is over $3000 so additional information written for and only readable by FinCEN (Financial Crimes Enforcement)

State Information? Example: New York State sales tax information for automation of state collected sales taxes

Erik Anderson
Bloomberg, X9 & W3C Web Payments

Many Different Identities

Erik Anderson
Bloomberg, X9 & W3C
Web Payments



consistof

Attribute
& Identifiers

correspondto

Identities

Entities

Facebook
Account

Target Loyalty
Card

Bank Account

Utility Bill

Geolocation

Asset Photos

Legal Entity
Identifier

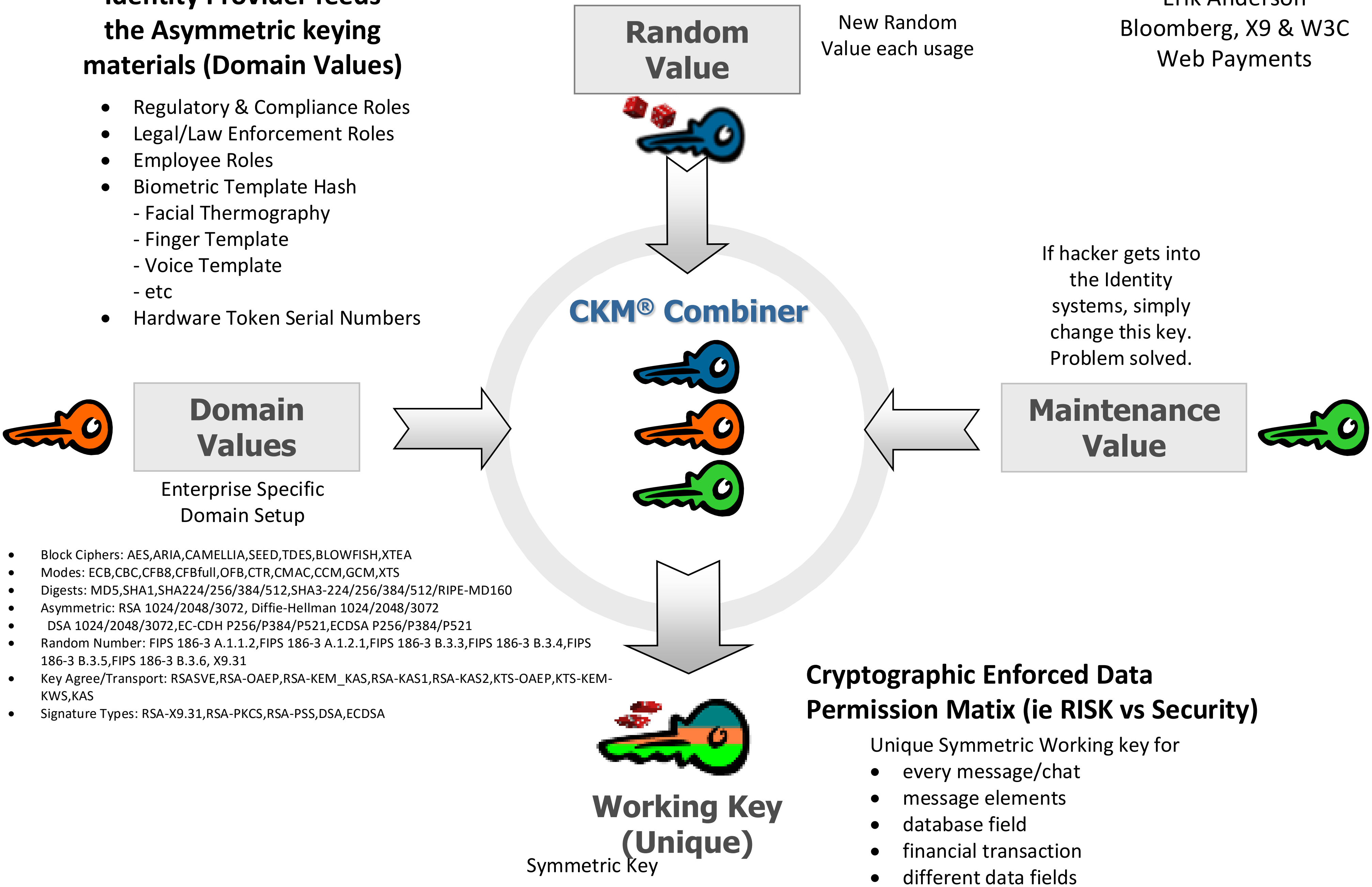
Credit Profile

Identity Provider (IdP) Key Construction & Materials

Identity Provider feeds the Asymmetric keying materials (Domain Values)

- Regulatory & Compliance Roles
- Legal/Law Enforcement Roles
- Employee Roles
- Biometric Template Hash
  - Facial Thermography
  - Finger Template
  - Voice Template
  - etc
- Hardware Token Serial Numbers

Erik Anderson
Bloomberg, X9 & W3C
Web Payments



Random Value

New Random Value each usage

CKM® Combiner

If hacker gets into the Identity systems, simply change this key. Problem solved.

Domain Values

Enterprise Specific Domain Setup

Maintenance Value

Working Key (Unique)

Symmetric Key

- Block Ciphers: AES,ARIA,CAMELLIA,SEED,TDES,BLOWFISH,XTEA
- Modes: ECB,CBC,CFB8,CFBfull,OFB,CTR,CMAC,CCM,GCM,XTS
- Digests: MD5,SHA1,SHA224/256/384/512,SHA3-224/256/384/512/RIPE-MD160
- Asymmetric: RSA 1024/2048/3072, Diffie-Hellman 1024/2048/3072
- DSA 1024/2048/3072,EC-CDH P256/P384/P521,ECDSA P256/P384/P521
- Random Number: FIPS 186-3 A.1.1.2,FIPS 186-3 A.1.2.1,FIPS 186-3 B.3.3,FIPS 186-3 B.3.4,FIPS 186-3 B.3.5,FIPS 186-3 B.3.6, X9.31
- Key Agree/Transport: RSASVE,RSA-OAEP,RSA-KEM_KAS,RSA-KAS1,RSA-KAS2,KTS-OAEP,KTS-KEM-KWS,KAS
- Signature Types: RSA-X9.31,RSA-PKCS,RSA-PSS,DSA,ECDSA

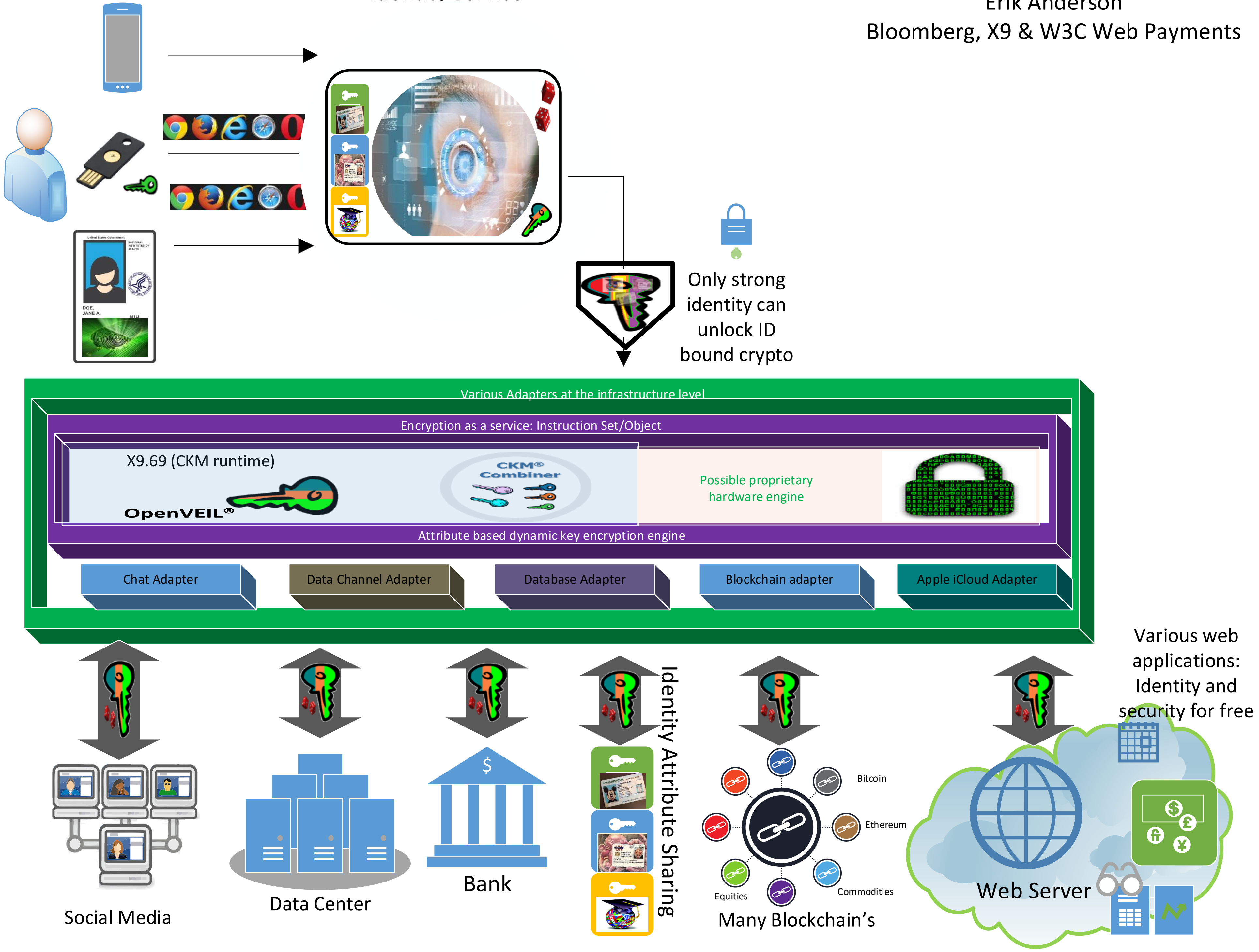
Cryptographic Enforced Data Permission Matix (ie RISK vs Security)

Unique Symmetric Working key for

- every message/chat
- message elements
- database field
- financial transaction
- different data fields
- Need to Know basis

Identity Service

Erik Anderson
Bloomberg, X9 & W3C Web Payments



Only strong identity can unlock ID bound crypto

Various Adapters at the infrastructure level

Encryption as a service: Instruction Set/Object

X9.69 (CKM runtime)

Possible proprietary hardware engine

Attribute based dynamic key encryption engine

Chat Adapter

Data Channel Adapter

Database Adapter

Blockchain adapter

Apple iCloud Adapter

Various web applications: Identity and security for free

Identity Attribute Sharing

Social Media

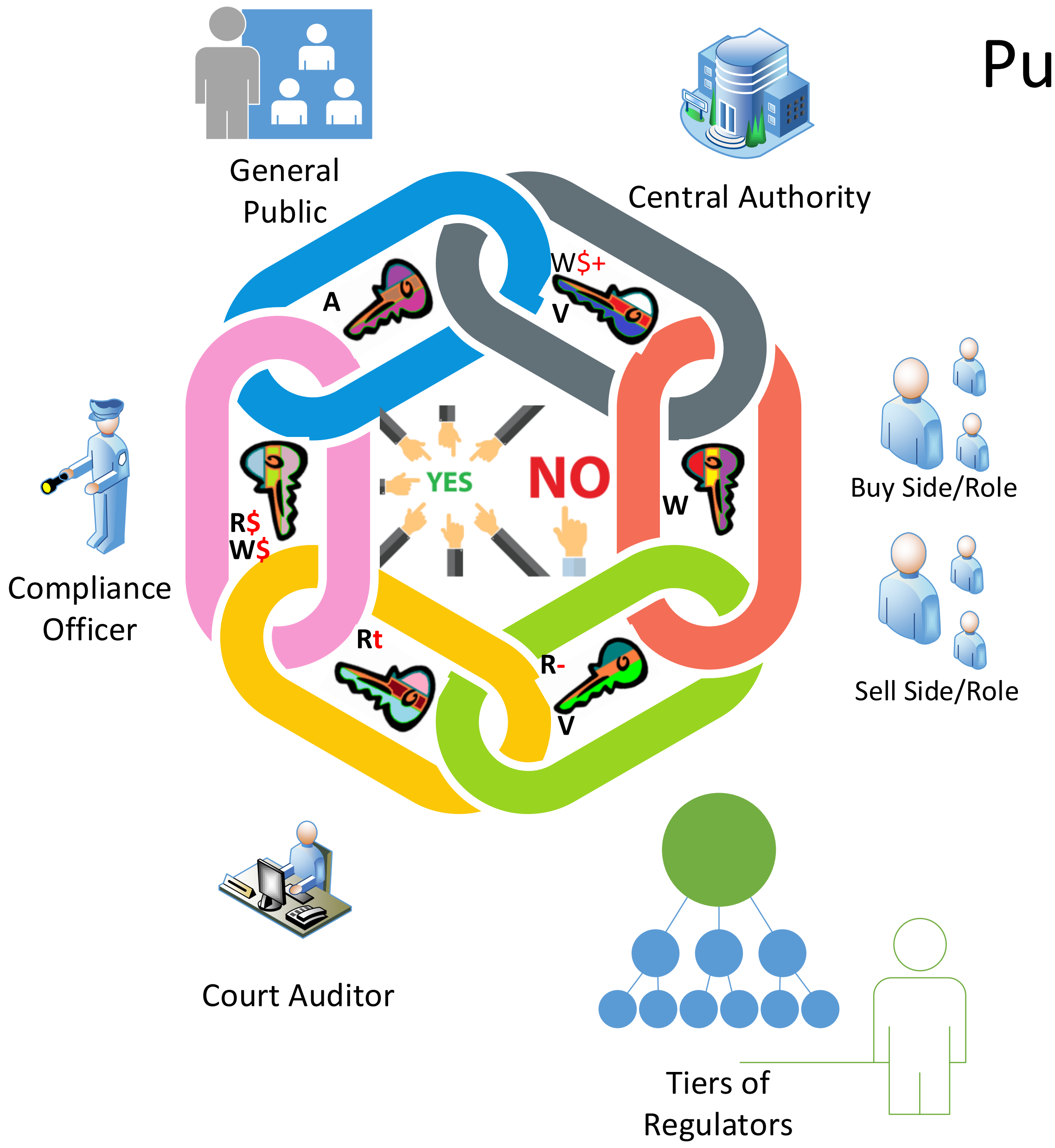
Data Center

Bank

Many Blockchain's

Web Server

Role Based Permissioned Public Blockchain&Ledger



A = Anonymous. Can see the transactions but no details.

W = Write access to the Blockchain

R- = Requests permission to read a transaction details.

Rt = Time based access to read all transaction details (Firm based). Times out after xx time.

R = Full read access (Allows regulatory snooping). Role based for a firm's transactions.

R$ = Can read all of its firms transaction & details.

W$ = Can countersign all of its firms transactions.

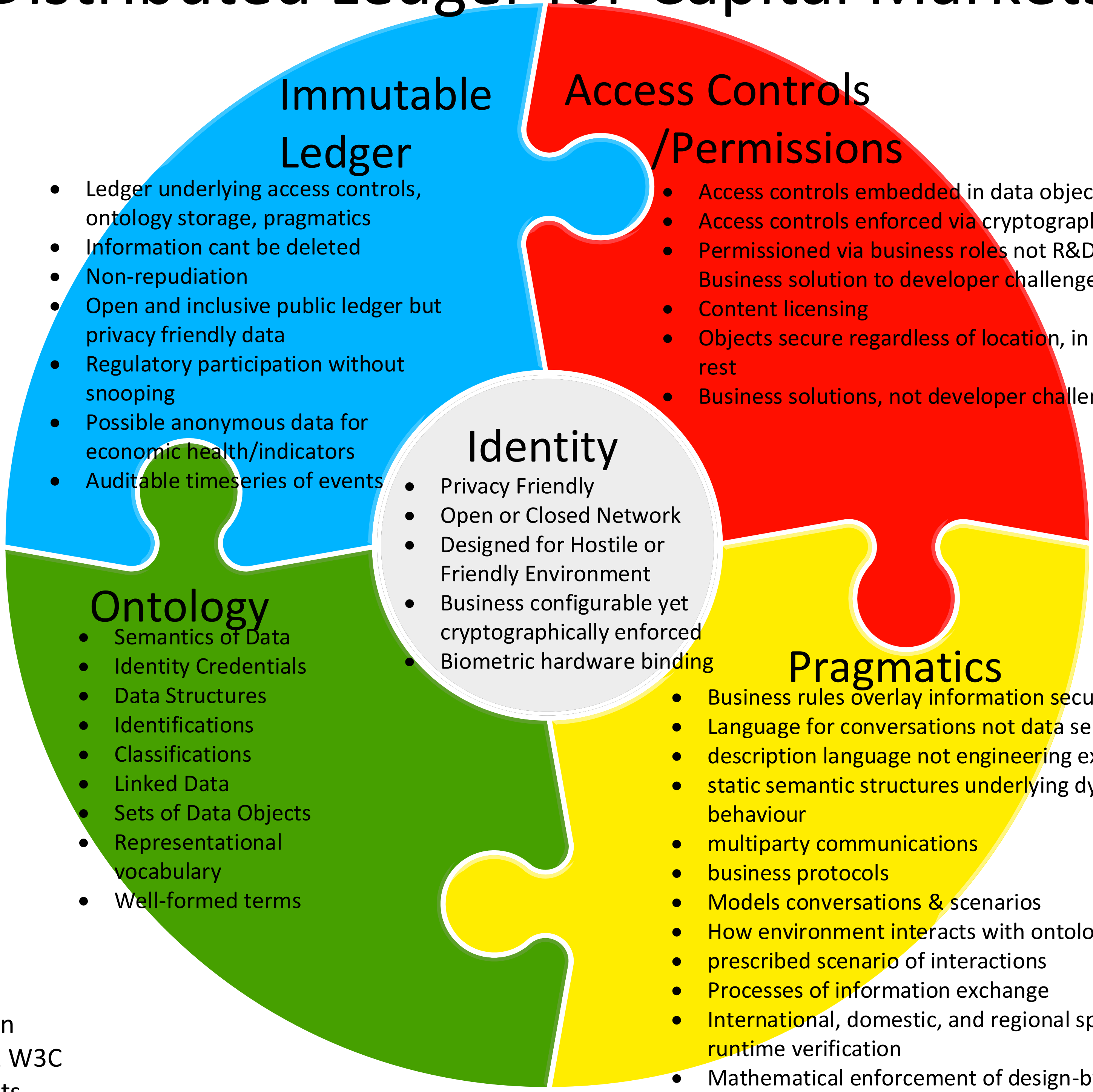
W$+ = Can countersign any transactions (or classification of transactions)

R$- = Can read all transactions (or a category of transactions)

V = Can validate an asset all the way back to its roots but cannot see the details of a transaction.

Erik Anderson
Bloomberg, X9 & W3C
Web Payments

Distributed Ledger for Capital Markets



Immutable Ledger

- Ledger underlying access controls, ontology storage, pragmatics
- Information cant be deleted
- Non-repudiation
- Open and inclusive public ledger but privacy friendly data
- Regulatory participation without snooping
- Possible anonymous data for economic health/indicators
- Auditable timeseries of events

Access Controls /Permissions

- Access controls embedded in data objects
- Access controls enforced via cryptography
- Permissioned via business roles not R&D programmers. Business solution to developer challenges.
- Content licensing
- Objects secure regardless of location, in motion, or at rest
- Business solutions, not developer challenges

Identity

- Privacy Friendly
- Open or Closed Network
- Designed for Hostile or Friendly Environment
- Business configurable yet cryptographically enforced
- Biometric hardware binding

Ontology

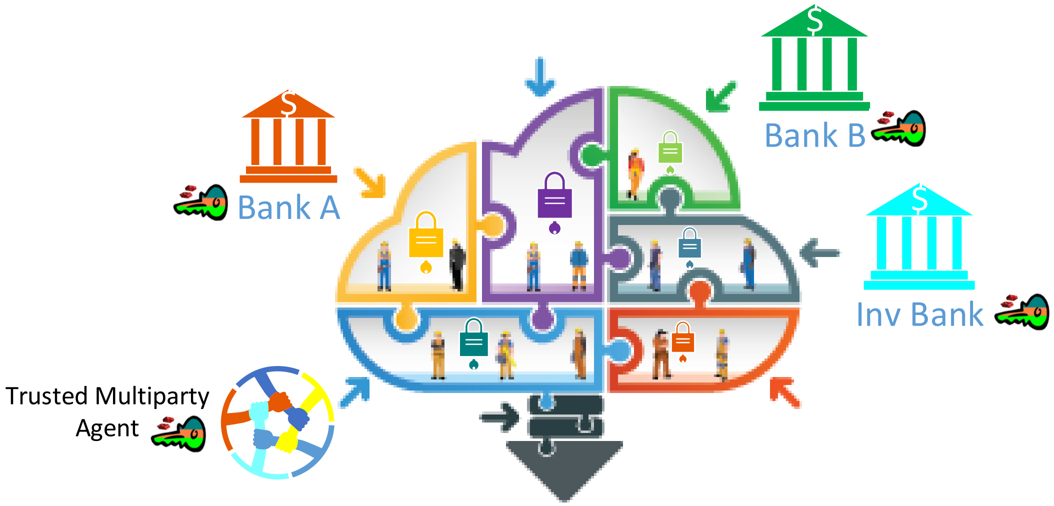
- Semantics of Data
- Identity Credentials
- Data Structures
- Identifications
- Classifications
- Linked Data
- Sets of Data Objects
- Representational vocabulary
- Well-formed terms

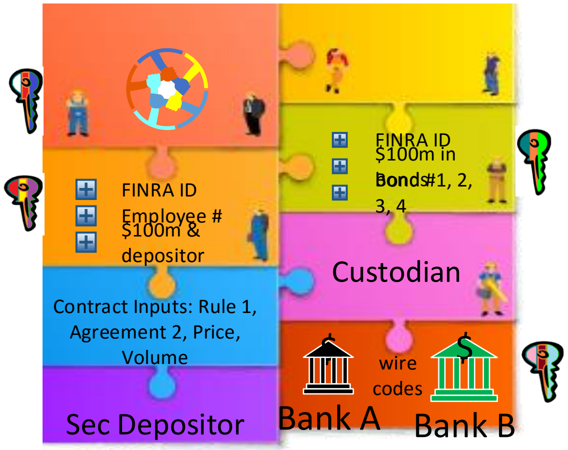
Pragmatics

- Business rules overlay information security engine
- Language for conversations not data semantics
- description language not engineering execution language
- static semantic structures underlying dynamic pragmatic behaviour
- multiparty communications
- business protocols
- Models conversations & scenarios
- How environment interacts with ontology
- prescribed scenario of interactions
- Processes of information exchange
- International, domestic, and regional specification to local runtime verification
- Mathematical enforcement of design-by-contract framework for business behaviors

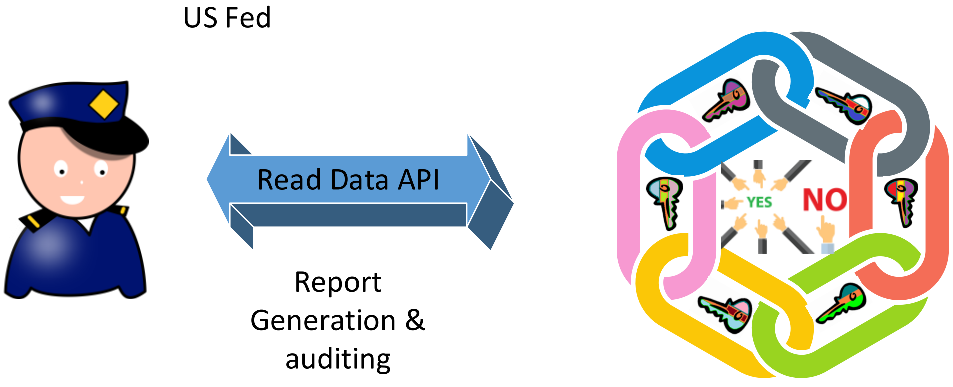
Erik Anderson
Bloomberg, X9 & W3C
Web Payments

Trades





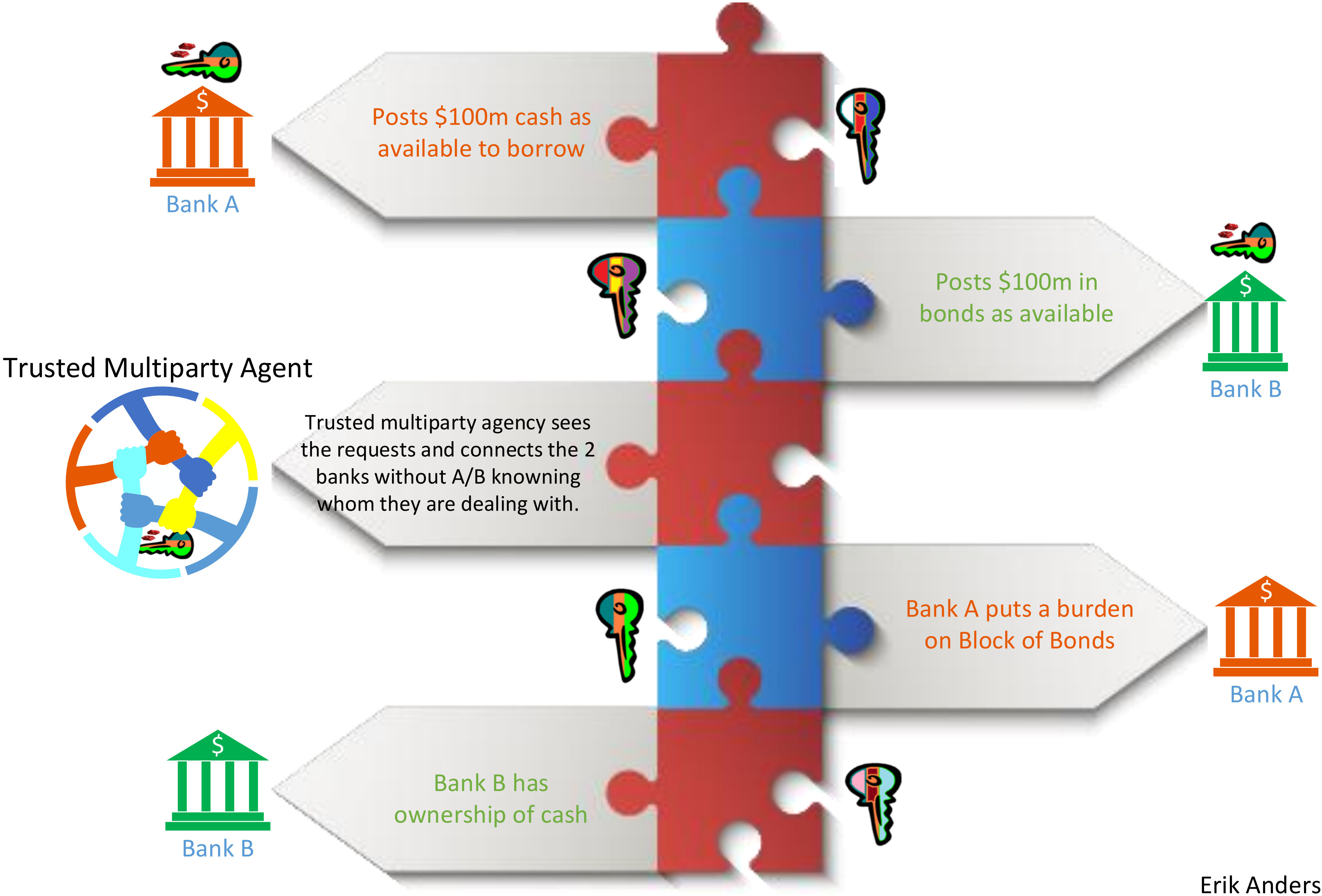
Information Sequence, Identities, Agreements, and Rules repackaged for public ledger storage.



Permissioned Public Ledger

Erik Anderson
Bloomberg, X9 & W3C
Web Payments

Information Sequencing



Bank A

Posts $100m cash as available to borrow

Posts $100m in bonds as available

Bank B

Trusted Multiparty Agent

Trusted multiparty agency sees the requests and connects the 2 banks without A/B knowning whom they are dealing with.

Bank A puts a burden on Block of Bonds

Bank A

Bank B

Bank B has ownership of cash

Erik Anderson
Bloomberg, X9 & W3C
Web Payments