

Identity and Payments

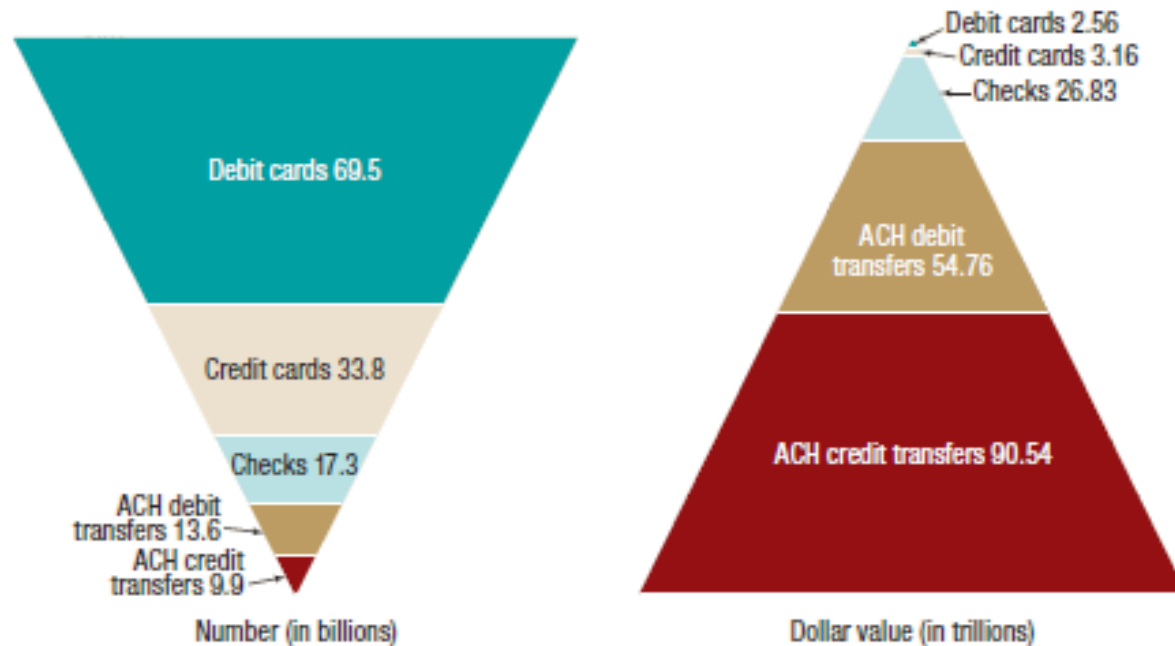
US Payment Forum
New Orleans
December 5th, 2017
Philip@Andreae.com

What are Payments



The Electronic Payment Landscape

Figure 1. Distribution of core noncash payments by type, number, and value, 2015



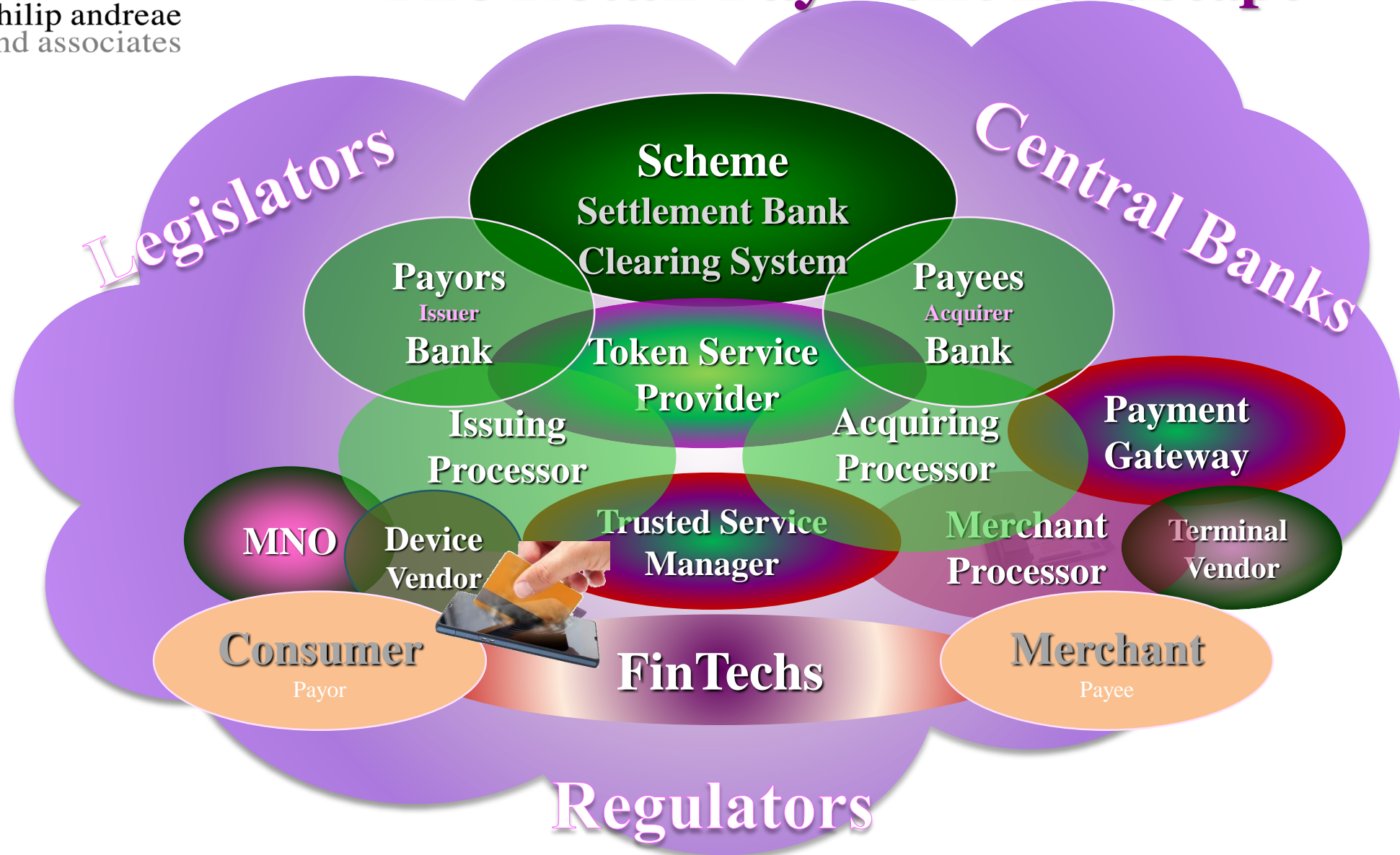
Note: Debit card includes non-prepaid debit, general-purpose prepaid, private-label prepaid, and electronic benefit transfers. Credit card includes general purpose and private label. Check, automated clearinghouse (ACH) credit transfers, and ACH debit transfers include interbank and on-us.

Federal Reserve Triannual Report on Payments.

Electronic Payments Are Based Multi Party Agreements



The Retail Payment Landscape



The Faster Payments Task Force

Anatomy of a Payment Focuses on Identity

TABLE 2: ANATOMY OF A PAYMENT

INITIATION	The initiation of a payment begins when either the payer or payee in a payment transaction, or a third party, sends an instruction to another entity that triggers a process ultimately leading to a payment.
AUTHENTICATION	The process that verifies the identity or veracity of a participant, device, payment or message connected to a payment system.
	Authentication may happen at multiple points in the payment process. For example: <ul style="list-style-type: none"> •End-user identity may be verified when the end user enrolls with a provider. •During the payment process, additional checks may be built in to verify the identity of the payer, account, or account provider (e.g., entering a password).
AUTHORIZATION	The explicit instructions, including timing, amount, payee, source of funds and other conditions given by the payer to their account provider or to the payee to transfer funds on a one-time or recurring basis.
APPROVAL BY THE PAYER'S PROVIDER	The point following the initiation of a payment when the payer's account provider verifies that the payer's account has good funds ¹³ or credit necessary to complete the transaction.
CLEARING	The process by which the payer's and payee's account providers exchange payment information to confirm a transaction prior to settlement.
RECEIPT	The point when funds are received by the payee, such that the funds can be withdrawn or transferred. ¹⁴
SETTLEMENT	An act that discharges obligations in respect of funds between two or more entities. ¹⁵
RECONCILIATION	A procedure to verify that the records issued by entities involved in a transaction match. The reconciliation process may include appropriate reversals and post-transaction analysis.

Authentication or better said Identification

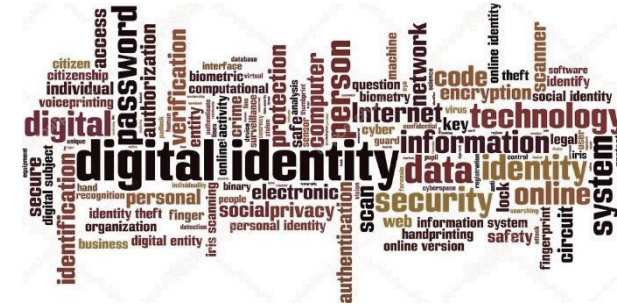
The process that verifies the identity or veracity of a participant, device, payment or message connected to a payment system.

What's In An Identity



Account Number

EMAIL Address



Alias

Pseudonym

User Name

What Is The Root of Trust For an Identity



Who Can We Trust Who Do They Trust

Government
Federal - State - City

AFGMA
Apple, Facebook, Google
Microsoft, Amazon

Utilities
Water, Electric, Cable, Gas

**Financial
Institution**

MNO



Users Seek to Enroll Anywhere

In Branch



Online



What Forms a Proof of Identity

Proof Provided by Others



Data Accumulated by Others



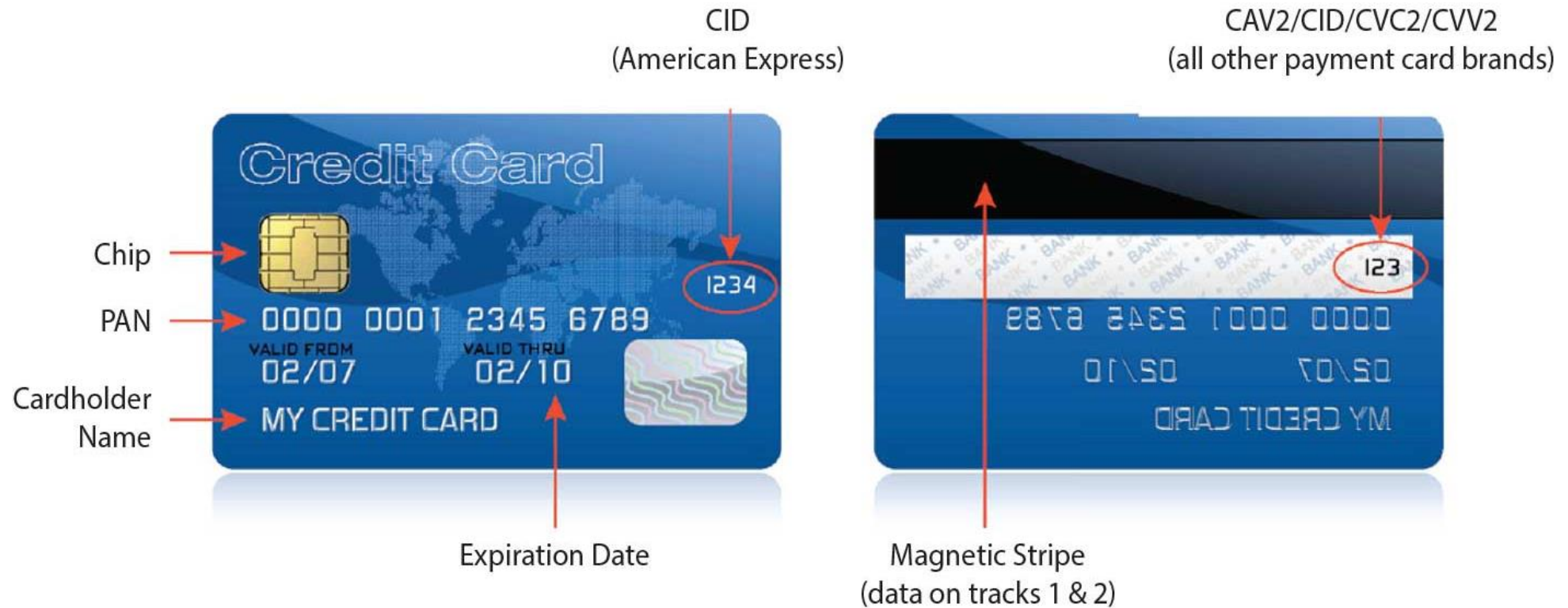
Payments Require Identity



ISO 7810, 7811, 7813

Defined a Means of Identification

The ID-1 Card

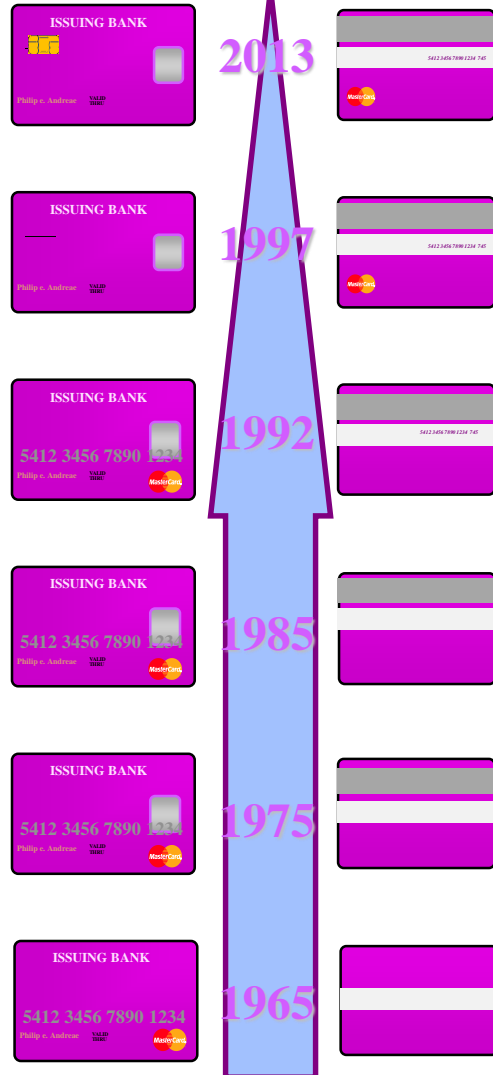


The Magnetic Stripe Made Our Identity Machine Read

Symbol	Description – Track 1 Structure	Character Code / Number of Characters
STX	Start Sentinel	%
FC	Format Code	B
PAN	Personal Account Number	Up to 19 Digits
FS	Separator	^
NM	Name surname surname separator first name or initial space when required middle name or initial period (when followed by title) Title (when used)	2 to 26 characters / Space .
FS	Separator	^
ED	Expiration date	Four digits or ^
SC	Service Code	Three digits of ^
DD	Discretionary data	Balance of characters
ETX	End Sentinel	?
LRC	Longitudinal redundancy check	1 character
	Maximum record length	79 alphanumeric characters

In The Physical World There Are Layers of Security





Payment Card Fraud Prevention Layering Security on to the Card

Card, Embossing, Magstripe, Hologram, CVC, Chip & Tokens

Card, Embossing, Magstripe, Hologram, CVC & Chip

Card, Embossing, Magstripe, Hologram & CVC

Card, Embossing, Magstripe & Hologram

Card, Embossing & Magstripe

Card, Embossing

What You Have
A CAM

Card Authentication Method
Credential Authentication Method

ISO 7816 & EMV Introduced Secure Elements & Cryptography to Assure Authentication

Simple Truths

- The Issuer assured our identity
- The PAN identifies our Means of Payment
- Data & cryptography converts cards into credentials
- Secrets and certificates assures the credential is unique
- Signature or PIN, Now Biometrics, verifies the presenter

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

Counterfeit Protection

Merchant Authentication
Card Risk Management
Issuer Authentication



Lost and Stolen Fraud
Cardholder Verification

Form Factor Independent
Contact, NFC or QR Code

Multi Factor Authentication

The Key to Secure Identification

- **Something You Have** ✓ **A Card or Token**
- **Something You Know** ✓ **PIN/Password**
- **Something You Are** ✓ **A Biometric**

CAM

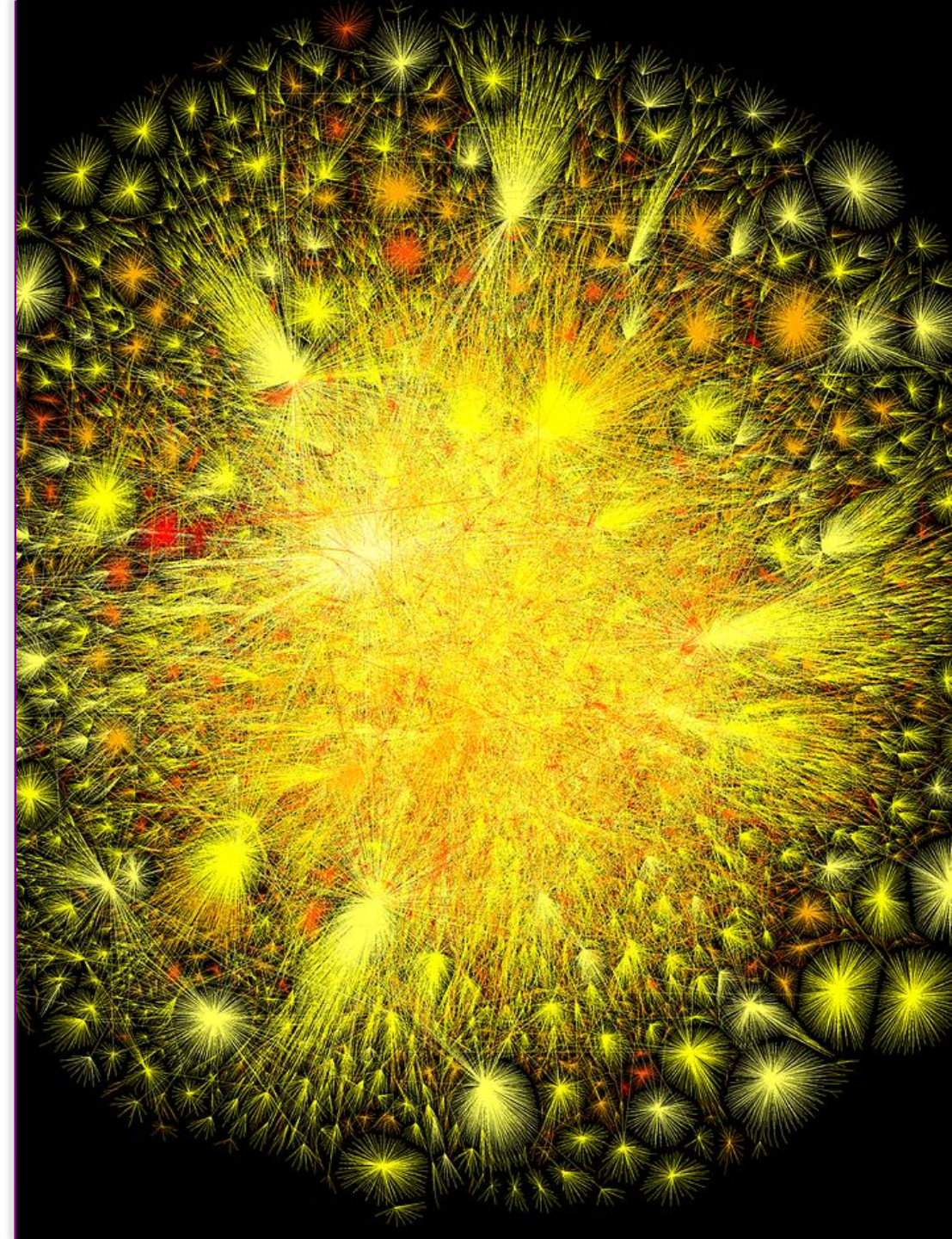
Credential Authentication Method

CVM

Cardholder Verification Method

To Reap the Benefits of the Internet

The Internet at the MOMA



Required a Means of Authentication

The Payment Schemes Tried

- STT, SEPP & SET

Were feeble attempts

- 3D-Secure 1.x

Fraught with challenges and ~~passwords~~



Our Payment Identifiers Became Sensitive Personal Information

- E2E or P2P Encryption
To protect data in motion
- Tokens and encrypted databases
To protect data at rest

All while EMV was being deployed

We Abandon Authentication

For Profit & Convenience

The New Yorker 1994



The New Yorker

"On the Internet, nobody knows you're a dog."

And They Came & Profited



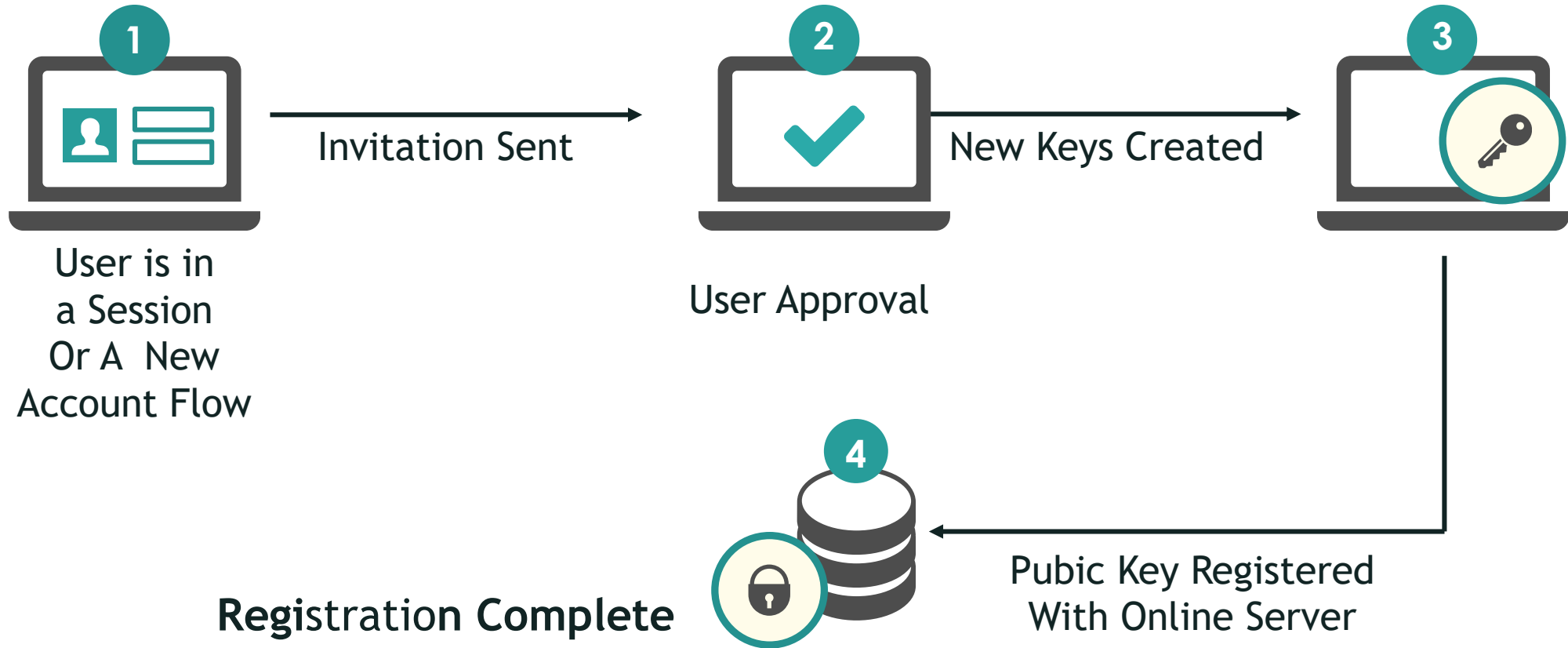
The Standards for Authentication Are Available

**ONLINE
AUTHENTICATION
USING
PUBLIC KEY
CRYPTOGRAPHY**

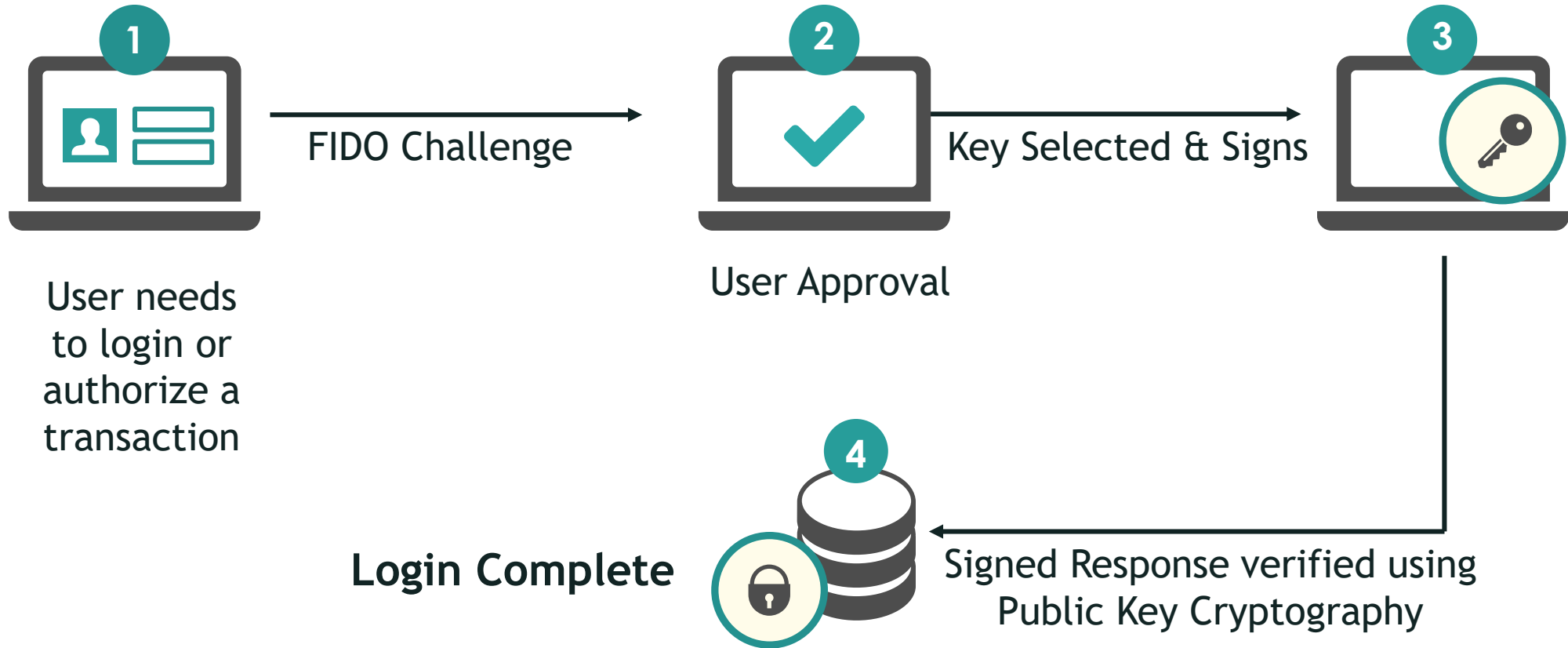
FIDO Cross-Platform Support



FIDO Registration

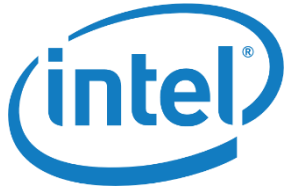


FIDO Authentication



FIDO IN THE WINDOWS + WEB ECOSYSTEMS

Windows Platforms



Lenovo
Yoga 910



Windows 10

Web



mozilla
Firefox



Microsoft Edge



Its All In The Words



- The identity of the fingerprints on the gun with those on file provided evidence that he was the killer.*

- the condition of being oneself or itself, and not another:

He began to doubt his own identity.

- condition or character as to who a person or what a thing is; the qualities, beliefs, etc., that distinguish or identify a person or thing:

a case of mistaken identity; a male gender identity; immigrants with strong ethnic identities.

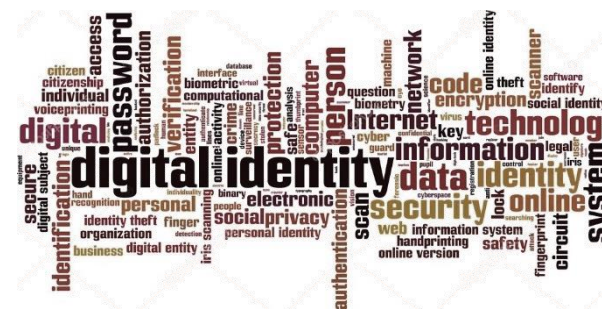
- the state or fact of being the same one as described.
- the sense of self, providing sameness and continuity in personality over time and sometimes disturbed in mental illnesses, as schizophrenia.

Identity

Account Number

First & Last Name

User Name



Driver License

Social Security Number

EMAIL Address

Authentication

Authenticate (verb)

to establish as genuine.

to establish the authorship or origin of conclusively or unquestionably, chiefly by the techniques of scholarship:

to authenticate a painting.



Identification

noun

an act or instance of identifying; the state of being identified.

something that identifies a person, animal, or thing:

He carries identification with him at all times.

Sociology. acceptance as one's own of the values and interests of a social group.

Psychology.

a process by which one ascribes to oneself the qualities or characteristics of another person.

(in psychoanalytic theory) the transference or reaction to one person with the feelings or responses relevant to another, as the identification of a teacher with a parent.

perception of another as an extension of oneself.



Authorization

Noun - the act of authorizing.

permission or power granted by an authority; sanction.

a legislative act authorizing money to be spent for government programs that specifies a maximum spending level without provision for actual funds.

a legislative act authorizing money to be spent for government programs that specifies a maximum spending level without provision for actual funds.



Identity

Authentication

Four Words

Independent and Inseparable

Identification

Authorization

Set Against Another Set of Words



Security

Noun

freedom from danger, risk, etc.; safety.
freedom from care, anxiety, or doubt;
well-founded confidence.

something that secures or makes safe;
protection; defense.

precautions taken to guard against crime, attack, sabotage, espionage, etc.: claims that security was lax at the embassy; the importance of computer security to prevent hackers from gaining access. an assurance; guarantee.



Confidentiality

(Noun)

Confidential - adjective

spoken, written, acted on, etc., in strict privacy or secrecy; secret:

a confidential remark.

indicating confidence or intimacy; imparting private matters:

a confidential tone of voice.

having another's trust or confidence; entrusted with secrets or private affairs:

a confidential secretary.

- bearing the classification confidential, usually being above restricted and below secret.
- limited to persons authorized to use information, documents, etc., so classified.



Privacy

Security

Three Concerns

Lost as we engage and leave tracks

Confidentiality

In Conclusion

**Electronic
Payments & Identity
Are inexplicitly
linked**



An Irrefutable Payment Is the Ultimate Requirement

Adjective

not capable of being refuted or
disproved

Synonyms

indisputable, incontrovertible,
undeniable

To assure the irrefutability of a payment

It is essential all parties:

- Are properly **identified** and therefore **authenticated**
- Agree and accept the terms of payment

And

- The payment is **authorized** by the payer and their financial institution
- The payment is accepted by the payee and its financial Institution

The funds move quickly from the Payor
to the Payee

Is Tokenization the Cure

Security Tokens

- Designed to address the PCI “Data at Rest” concern
- Removes PII data from the merchant’s environment
- Enables merchants to research, report and otherwise manage payments, exception, refunds and returns

Payment Tokens

- Designed to address the challenges created by the inability to support authentication on the Internet
- Adheres to the ISO 7812 principles of the PAN with BIN, Account Number and check digit capable to identify network, issuer and product
- Limits exposure of card data
- Provides segregation of transaction by device and potentially person
- Same yet different to what some call an alternate PAN or Alias PAN

