

Digital Identity

Today's Challenge Yesterday's Mistake

Four Words and Three Concerns as We
Think About The Issue Of Digital Identity

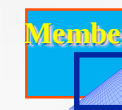


Philip Andreae



Helps the visually impaired

MCGILCHY NEWSPAPERS



The Card was a Secure Token

A Laminated Sandwich with Security On & In It

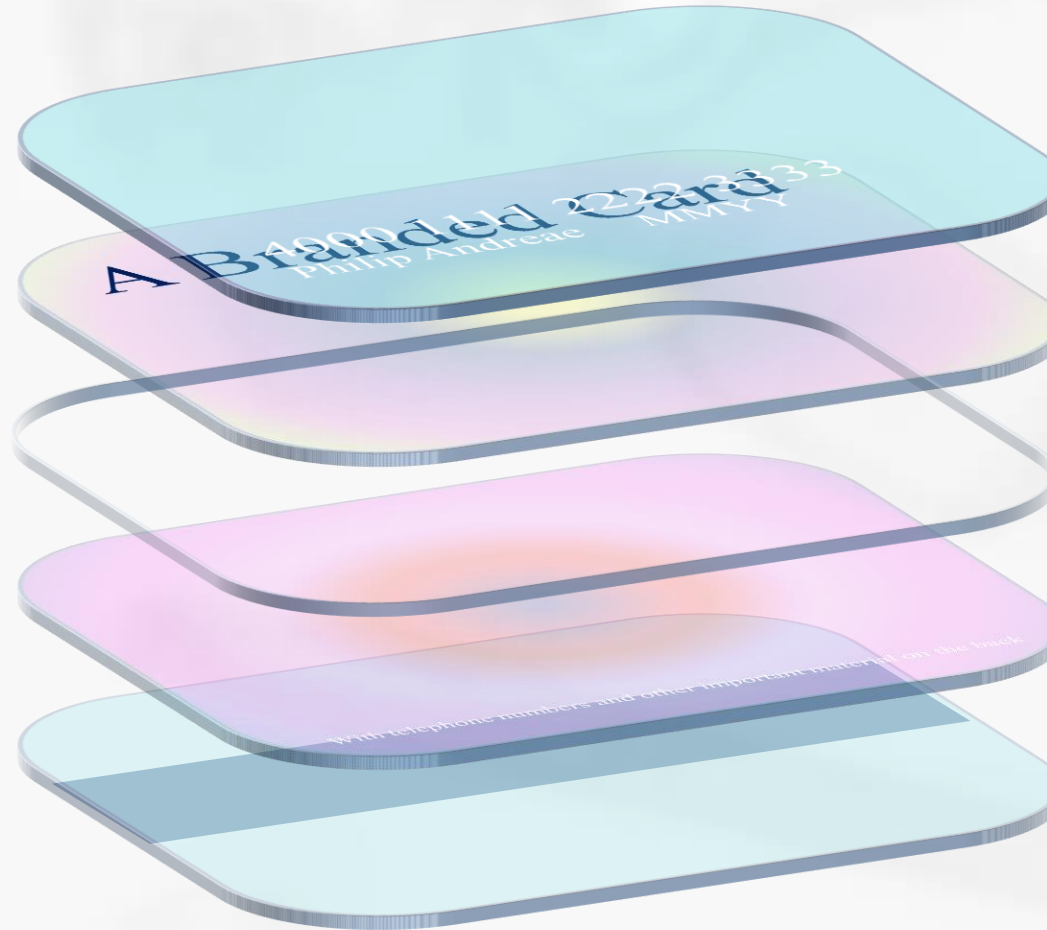
Clear
Laminate

Front

Inlay

Back

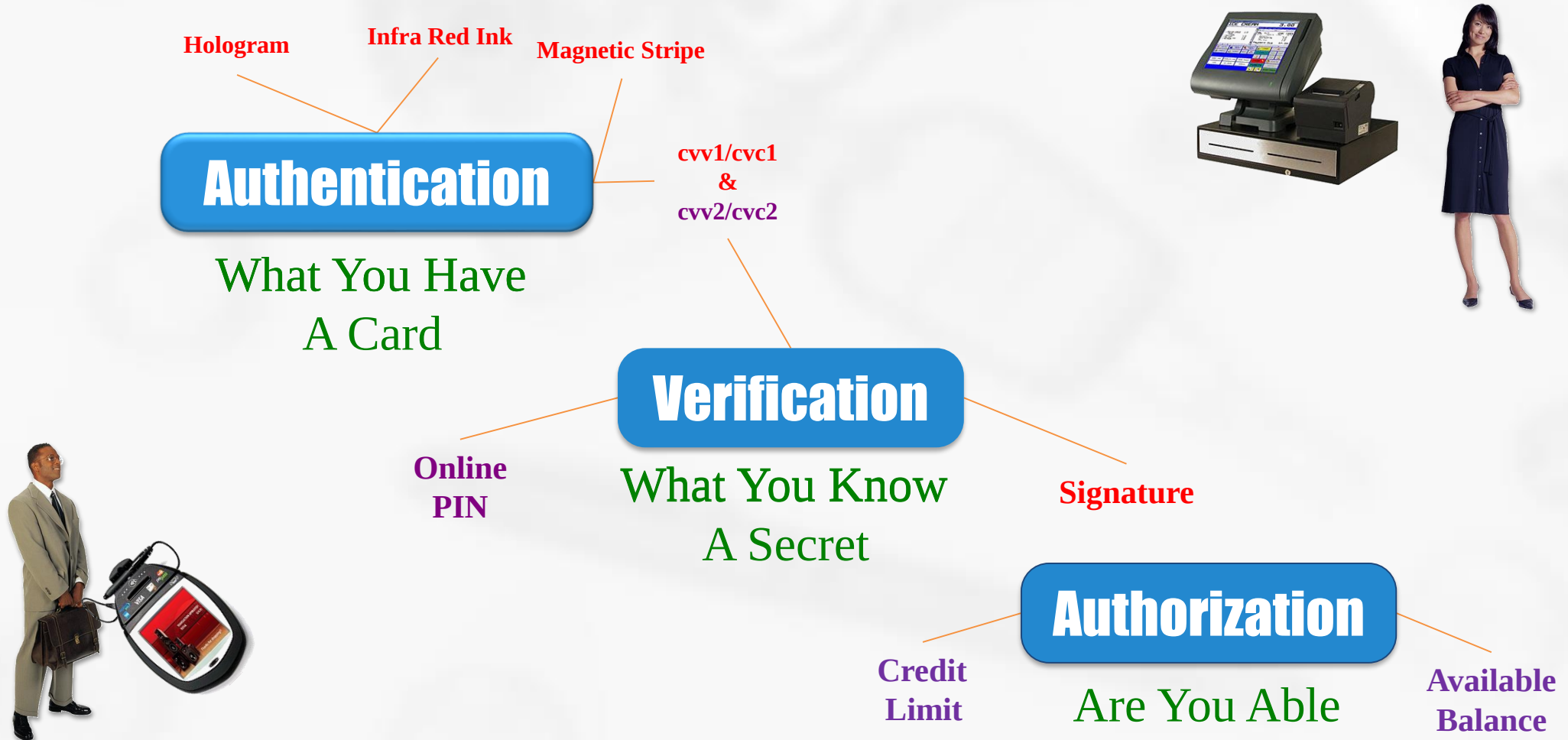
Clear Laminate
Magnetic Stripe



Personalized
To Represent
A Person

Physical World of Cards

No Longer Secure Circa 1991



EUROPAY
International



MasterCard
Worldwide



EMV the Global Standard for Credit & Debit Payments

**In 1993 the International Payment Schemes Agreed
The Long Term Solution To Fraud Was The “ICC”**

**They Agreed To Develop A Common Specification
With the Goal of Global Interoperability**

**They Agreed the Requirements and Published Version 3 in 1996
“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

Offline Authorization
Cost Reduction



Lost and Stolen Fraud
Cardholder Verification

Revenue Creation
Value Added Services

ICC Architecture

An Integrated Circuit Inside a Card

Offering the Dip or Tap Feeling



ICC Architecture

An Integrated Circuit Inside a Phone

Offering the Dip or Tap Feeling

Antenna

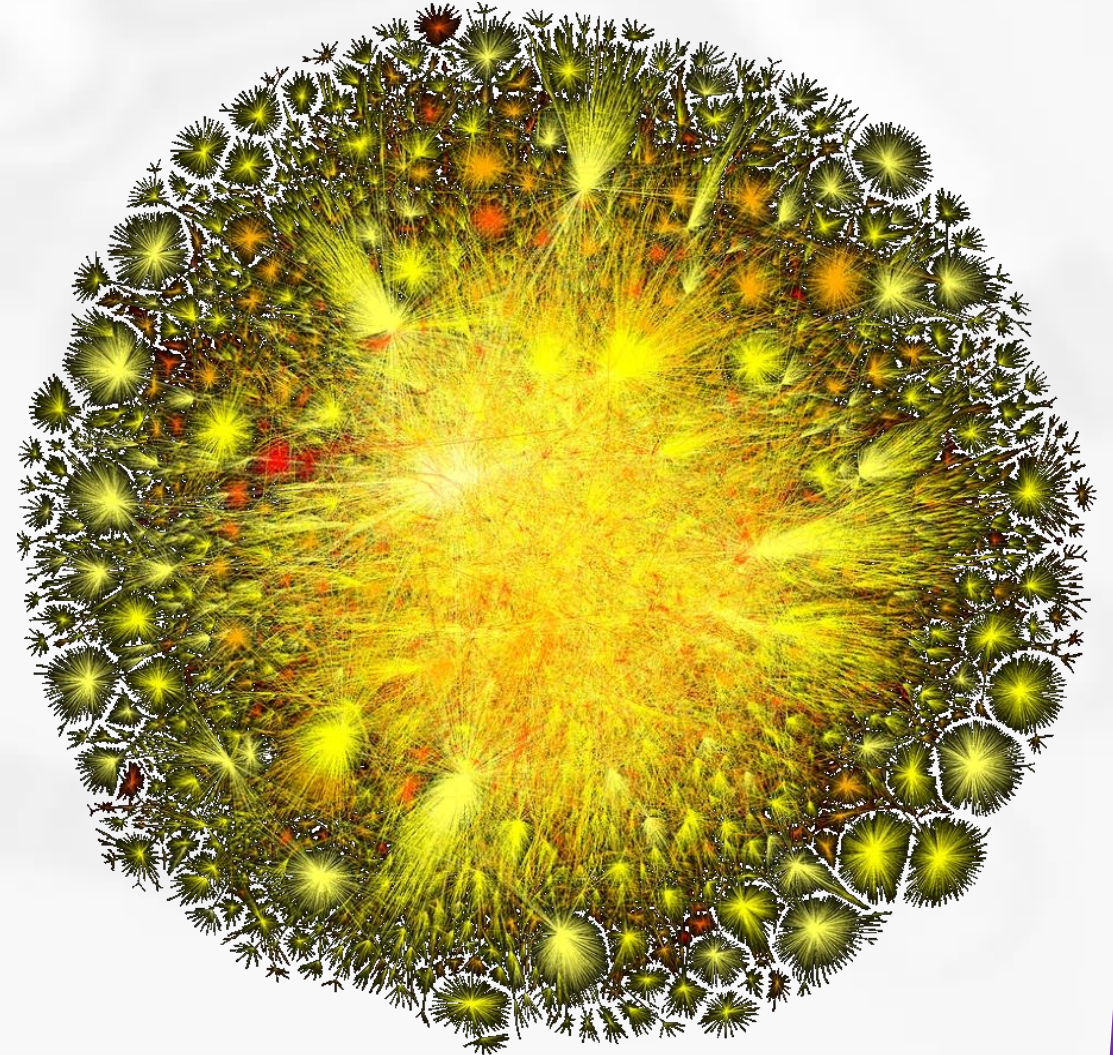


On the Internet, No One Know's You're a Dog



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

The New Yorker – Circa 1993

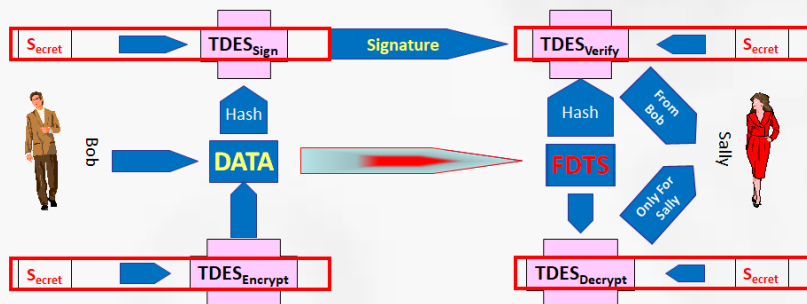


The Internet at the MOMA

To Assure Your Identity What You Need **Is** A Secure Element Inside

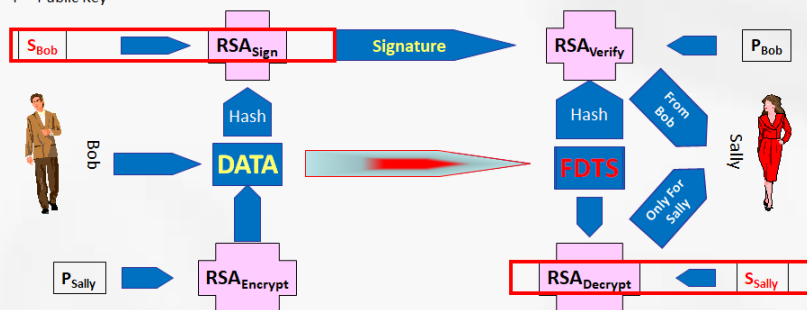
Symmetric

S – Secret Key



Asymmetric

S – Private Key
P – Public Key



The Integrated Circuit is:

- The chip on a card
- The Trusted Processing Module TPM in personal computers
- The secure enclave in an iPhone
- The secure element inside many devices
- The Trusted Execution Environment 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 ...

A Shared Secret

Online authentication

Public / Private Key Pairs(s)

RSA Elliptic Curves

No Shared Secret

Offline authentication

FIDO, W3C, WebAuthN & WebCrypto

NIST 800-63-3

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



**Layered Security
To Assure Identity**



**EMV, PIV, ICAO, eID,
WedAuthN, FIDO ...**



**User Name, Phone Number
As The Identifier**



**Hardware Secured Secrets
Biometric Sensors & The Power of Cryptography**



**A Biometric Authenticator
Assuring You are You**



Identifier

Authentication

Four Words

Independent and Inseparable

Identification

Authorization

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.

Social Security Number

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

He carries identification with him at all times.

Psychology.

(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.



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.



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.

Authentication Is the Easy Part

Enrollment

Identity Proofing

Registration

Transact



"Remember when, on the Internet, nobody knew who you were?"

Enroll

Proof

Four Steps

To Establish the Relationship

Register

Transact

The Relying Party

- Employer
- Government
- Service Provider
- Financial Institution
- Social Media
- Merchant
- Club

Enroll

Offers a Service via

- A Branch
- The Internet
- A Mobile App

Requests User Attributes

- Name
- Address
- Phone Number
- Social Security Number
- Drivers license
- Selfie
- Other pertinent data

GENERAL INFORMATION			
Name:		Nicknames:	
Current Age:	Gender:	Sexual preference:	
Number of siblings:	Your place in birth order:	Closest with which parent?	
Location:	Current level of study:	Current profession:	
Drug use/frequency and type?		Alcohol use/frequency and type?	
Languages spoken:		Number of current close friends: 0-2 3-8 9-15 16+ (please circle)	
What type of friendship are you looking for (best friend, close friend, friend with benefits, acquaintance, etc.)?			
PERSONALITY			
Circle the 5 which you think most describe you:			
<i>Adventurer; Animal Lover; Artsy; Athletic; Blogger; Blue Collar; Bookworm; Class Clown; Club Kid; Coffee Snob; Comic Nerd; Crafty; Daredevil; Diva; Fashionista; Film/TV Junkie; Free Thinker; Geek; Gamer; Hedonist; Hipster; Hippie; Homebody; Hopeless Romantic; Humanist; Intellectual; Maker; Music Snob; Night Owl; Nomad; Photographer; Player; Poet; Princess; Professional; Rockstar; Starving Artist; Straight Edge; Traveler; Techie; Treehugger; Sapiohille; Tattooed/Pierced; Vegetarian; Vegan; Yogi; Yuppy</i>			
Other(s): _____			
Choose two of those five traits and give a brief summary of how that choice plays a role in your life:			
1)			
2)			
List six main personality traits you have (3 positive, 3 negative)			
Rate your confidence (1-10):	Rate your happiness (1-10):	Rate your enjoyment of life (1-10):	
Rate your maturity level (1-10):	Mental disorders/types?		
Are you more logical or emotional?	Describe your sense of humour:		
OPINIONS AND VALUES			
Define "intelligence" in your own words:			
Political beliefs:		The world is getting better worse	
Religious/spiritual beliefs:		Love is overrated underrated neither	
The most important things in my life are:			
Tolerance for those who are different than yourself: complete tolerance high medium low complete lack (circle one)			
Willingness to make compromises: complete willingness high medium low complete lack (circle one)			
Patience when dealing with the flaws of others: complete patience high medium low complete lack (circle one)			
Rate the following using the numbers 1 to 5 (1 being of no importance to you, 3 being somewhat, 5 being of great importance)			
Honesty	Polite manners	Socializing	Time alone
Learning new things	Being kind	Getting what you want	Pleasing others
Have you ever stolen something?		Have you ever scammed someone?	
If you answered yes to either, please explain the situation and how you feel looking back on it:			
How important is fun in your life?		How much fun do you have in your life?	

Proofing

Identity Verification

Department of Motor Vehicles

State Department

USPS

Credit Bureaus

IRS

Identity Proofing

IAL

Identity Assurance Level

Utility Company

Phone Company

A Question of Risk

Social Media

Educational Institutes

FAL

Federated Assurance Level

Friends & Family

Financial Institutions

The process of proving the person is who they are

The moment when privileges and rights are defined

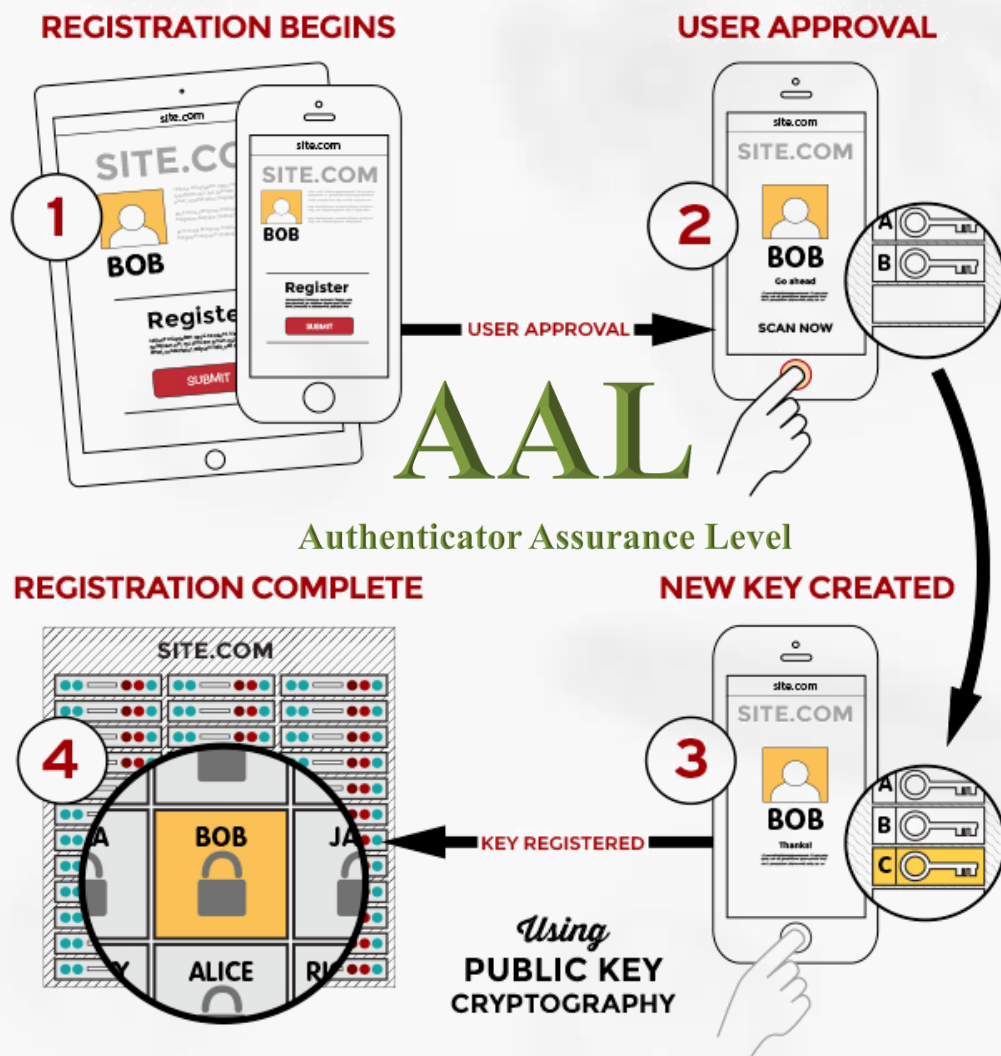
Synthetic Identity

Fraud

Lost & Stolen

Identity Theft

Registration



**The Relying Party
Is Convinced of Your Identity**

The User creates an Identifier

The User Registers the Authenticator

- Password was the authenticator
- Today the Authenticator should be a layered Multi-factor solution
 - What You Have
 - What You Are
 - What You Know

Designed to Assure Privacy

With a Limited Sharing of Attributes

**With an Appreciation of
The Right to be Forgotten**

An Effortless User experience

Log-in

- With your Identifier and Authenticator
- Assuring the relying party the same individual who registered is present

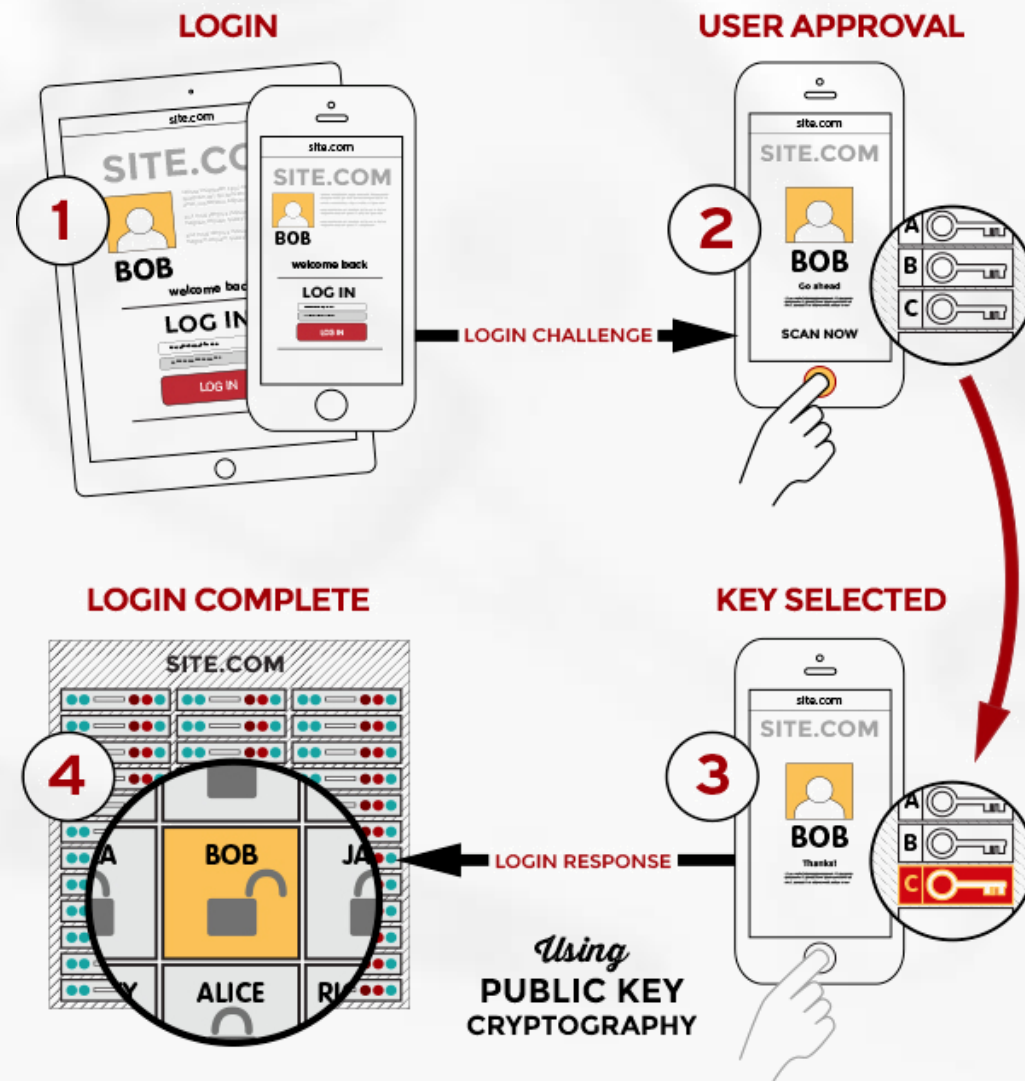
Step-Up

- When the risk associated with the transaction or event requires further confirmation of User Presence

Payments

- May involve counterparties seeking assurance of user presence

Transact



Three Concerns

Privacy

Security

Confidentiality

Lost as we engage and leave tracks



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.



Identity

Authentication

Four Words

Independent and Inseparable

Authorization

Identification

Identity

Authentication

Registration & Proof

Establishing Attributes and Defining Rights

Authorization

Identification

Identity

Authentication

Privacy

Security

Confidentiality

Authorization

Identification

Exploiting Cryptography Using Algorithms, Keys & Certificates To Assure Trust

Any Questions

Philip@Andreae.com

www.andreae.com

*Thank you for
your patience*

