Brewing Next Generation Identity

Kal Toth, P.Eng., Ph.D.

http://www.betterthanyourwallet.com

Pacific Northwest Software Quality Conference (PNSQC)
October 12-13, 2015

The Problem: On the Internet, nobody knows you're a dog

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

Peter Steiner's cartoon, as published in *The New Yorker, 7/5/1993*

Distinguishing collaborators from impersonators is a tough problem

If it was easy someone would have solved this by now

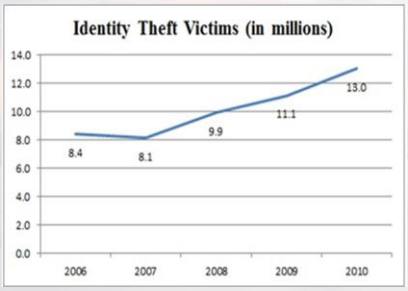
Ongoing Identity Problem

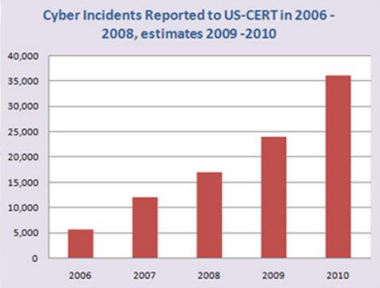
- ✓ Exponential Trend: Identity theft ↑ impersonation ↑ exploits ↑
- ✓ Numerous Causes: compromised passwords, phishing, malware, and breached servers and user devices

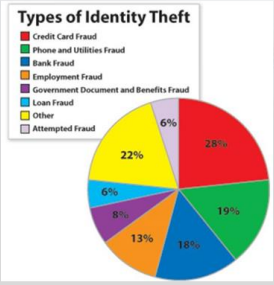
- ✓ At least $5.5B in losses in credit card fraud in 2012
- ✓ At least 500M personnel records breached in 2014
- ✓ At least 100M payment cards breached in 2014

- ✓ Identity solutions not keeping pace
- ✓ Do we have an identity crisis?

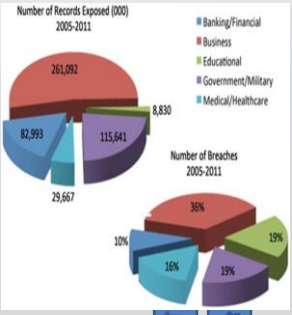
Scope and Scale of Identity Problem

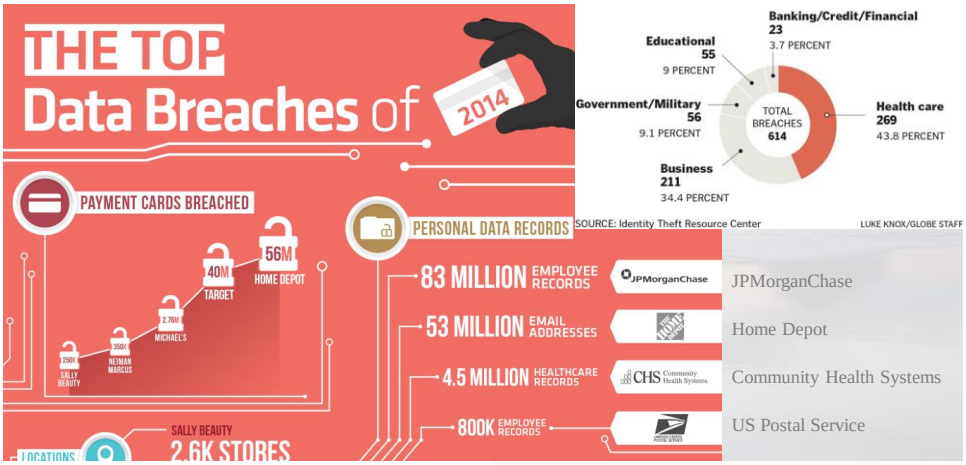






2012 Credit Card Fraud Statistics US Department of Justice 7-23-2012	
% US Victims of Credit Card Fraud	10%
% US Victims of debit or ATM Fraud	7%
% of Financial Fraud Related to Credit Cards	40%
Total Amount of Credit Card Fraud Worldwide	$5.55 B
% Fraud Originating from Email	48%
% Fraud Originating from Websites	12%





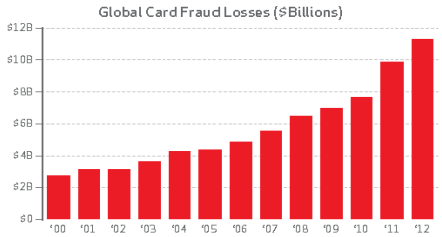
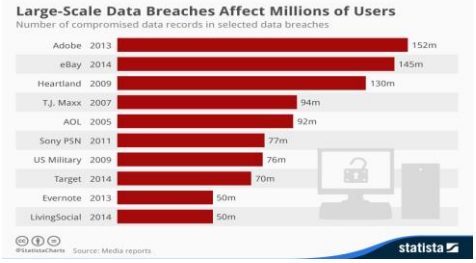
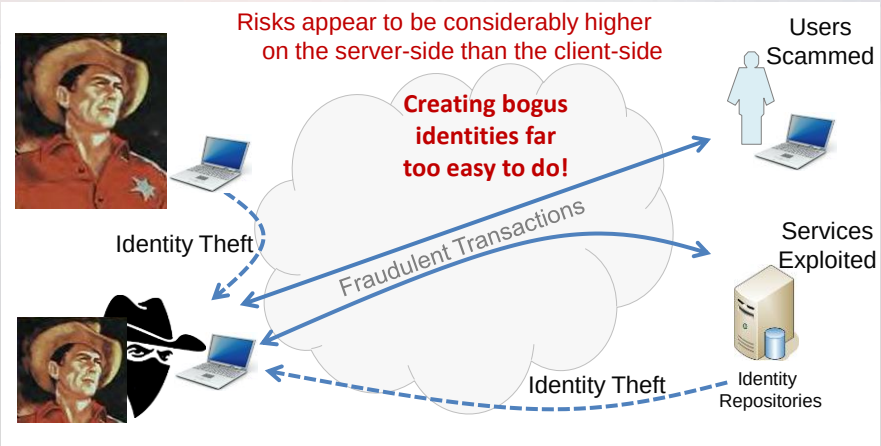


Figure 2: The cost of card fraud; data from The Nilson Report, August 2013



Simple Analysis: Identity Theft → Impersonation → Fraud

- Faulty identity, authentication and access specs, designs, implementations
- Identifying information stolen / copied
- Bogus physical and electronic credentials created
- Legitimate users impersonated
- Fraud committed



What can we do to solve this identity crisis?

- ✓ **Understand identity and identity provisioning better**
- ✓ **Distinguish between identity and authentication**
- ✓ **Portable Identities:** Create identities that can be used across the web (e.g. electronic drivers licenses, bank cards, business cards)
- ✓ **Multi-Factor Authentication:** Strongly bind users to identities and make them (1) much harder to steal and (2) prevent misuse
- ✓ **Biometrics:** leverage multiple biometric authentication factors
- ✓ **Multiple Attestation:** Enable multiple identity attestations to elevate identity assurances – central authorities **and** known-persons
- ✓ **Personal Devices:** leverage their powerful features more effectively
- ✓ **Existing identity solutions:** consider their strengths/weaknesses

Identity and Identity Provisioning

An identifier: an attribute only of a person

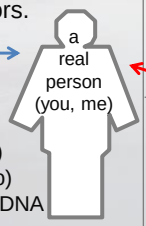
e.g. legal name, pen name (pseudonym), passport #, drivers license #, employee number, a social security number, …

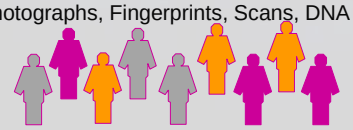
Passwords, PINs & private crypto keys are secrets of the user designed to prevent e-fraud … are not user identities

Digital Certificates:
- do not specify the owner's identity
- only selected attributes of the owner

Identity: Collection of personal attributes distinguishing a real person from "all" other persons including impersonators.

Personal Attributes
Identifiers
Physical characteristics
Life Events
Endorsements (qualified to do)
Restrictions (not permitted to do)
Photographs, Fingerprints, Scans, DNA





Credential: a physical document that
(1) specifies a person's identity
(2) attested to by another person.

"proofed"

E-Credentials are electronic equivalents of a physical credentials …
- specify person's identity (certain attributes)
- identities are attested to by 3rd party(ies)
- an identity attester should not be able to repudiate their attestation

Portable Electronic Identities

Multi-Factor Authentication [MFA]

Multiple identity verification factors authenticate the user:

- **Possession:** What the user has (authenticating HW token or personal device)
- **Knowledge:** What the user knows (like a PIN or password)
- **Biometric:** What the user is (finger, face, iris, hand, voice, heartbeat, etc.)

Combining Factors elevates Authentication Assurances

Authentication performed by (1) user's device or (2) provider's device

- Poses privacy risk if captured and processed by a provider device

Examples:

- **Chip/PIN Card:** banking smart card (2-factor)
- **OTP Token:** one-time-password generator (time, pseudo-random, QR code, …)
- **OOB (Out-of-Band) Authentication:** Mobile phone receives OTP password
- **FingerPrint Authenticator:** reads 1 or more finger prints and generates OTP

Biometric Authentication [BIO]

Examples	Face, finger, signature, voice, iris, heart, keying, venal, …
Technologies	Many algorithms, scanners, HW and SW solutions, …
Data [Ma]	False positives a significant challenge
	Face 43%, finger 30%, signature 28%, voice 20%, iris 4.7%
Benefits	Can be used to elevate authentication assurances
	Mitigate impersonation risk
IFF	Biometric reliably matches person's identifying info
	Biometric by itself only provides "same person" assurances

Observations:

- Individual preferences and constraints for biometric schemes vary (a lot)
- Biometric data must be strongly protected against tampering and theft
- Support for multiple biometrics is probably a good business strategy

Features of Personal Devices to Exploit

Smart Phones, Tablet PCs, Laptops

Cameras for facial and iris biometrics

Integrated fingerprint scanners

Handwriting and voice recognition?

Cameras to enable personal identity specification

NFC, Blue-Tooth and WiFi to safely exchange identities

Embedded crypto: authentication, privacy, attestation

Trusted execution: Intel, Samsung, BBRY

Reviewed Identity Technologies

[see annex]

1. Remote Access Passwords / PINs [P/P]
2. Federated Identity / Single-Sign-On [SSO]
3. Public Key Infrastructure + Client Certs [PKI]
4. Pretty Good Privacy + Client Certs [PGP]
5. Derived Credentials [DCRD]
6. Fast IDentity Online Authenticators [FIDO]

- Description
- Identity Specification, Proofing and Attestation
- Local Authentication
- Originator Authentication and Channel Privacy
- Private Keys
- Strengths
- Vulnerabilities

Next Generation Identity

Identity Technology Review (1)

A. General

- Remote password/PIN authentication widely considered to be inadequate for controlling access to sensitive and/or high value transactions.
- Identity theft and electronic fraud due to server-side repository breaches appears to dwarf the risks of client-side compromises.
- PGP designed to support secure collaboration among users (not with services).
- Other solutions reviewed enable secure client-server collaboration.

B. Identity Specification, Proofing and Attestation

- Only PGP supports a degree of mutual attestation by users.
- Other solutions rely on server-side procedures to capture, proof and attest user identities.
- PGP and PKI weakly specify client certificates; user identity proofing/attestation is generally not performed except in the case of Derived Credentials.
- FIDO does not capture, proof or attest the identity of users.

Identity Technology Review (2)

C. Local Authentication
- Remote password/PIN, SSO, PKI, PGP do not specify local user authentication
- Derived Credentials (via PIN) and FIDO (various) support multi-factor user authentication.

D. Remote Authentication and Encryption
- PKI, PGP and Derived Credentials deliver strong remote authentication and encryption using public/private key encryption technologies

E. Private Key Protection
- PKI and Derived Credential authorities distribute and retain users' private keys which could compromise transaction security.
- In contrast, PGP and FIDO prevent the disclosure of generated private keys.

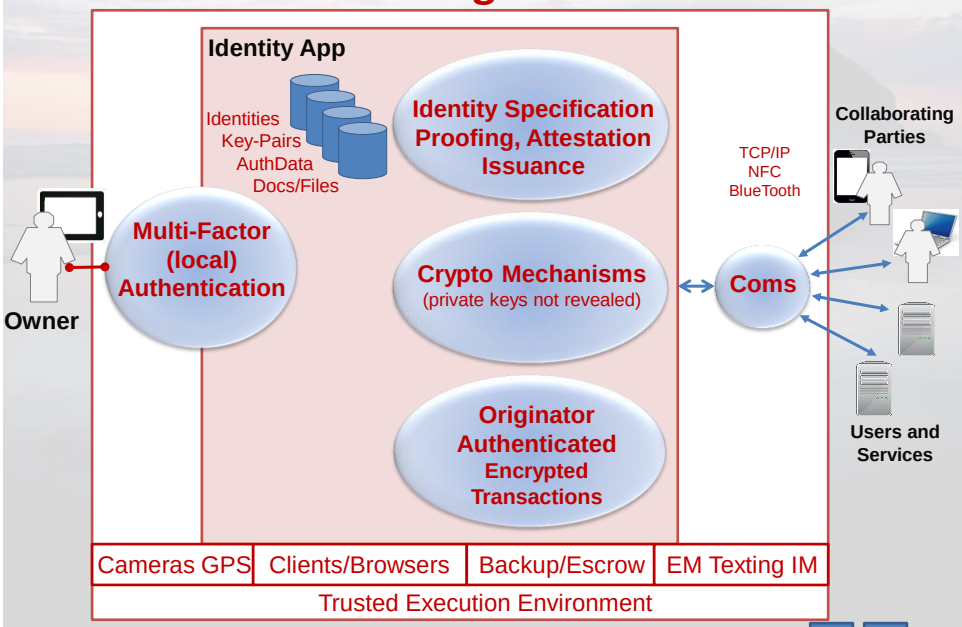
Next Generation Identity Characterized (1)

- **General:** Supports both client-server and user-to-user collaboration. Identity apps installed on personal devices enable local authentication, identity specification, proofing, attestation, issuance, and secure remote collaboration.
- **Identity Specification:** Identity owners and 3rd party authorities specify multiple identities for designated purposes.
- "True", anonymous and pseudo-anonymous identities supported.
- **Identity Proofing and Attestation:** Both collaborating users and identity authorities can proof, attest and issue user identities.
- **Proofing/Attestation** can be conducted in-person and/or online.
- **Identity Attestation:** Attestations are cryptographically bound to the identity of issuers – they cannot be repudiated.

Next Generation Identity Characterized (2)

- **Local Authentication:** Multiple authentication factors [MFA] including biometrics strongly bind the user to: (1) their identities, (2) private and public keys, and (3) remote collaboration mechanisms.
- **Secure Remote Collaboration:** Public/private key pairs associated with each user identity are used to authenticate/encrypt remote transactions.
- **Private Keys:** Private keys bound to an owner's identity are not revealed to relying parties.
- **Important Notes:** Without the user's private keys, identity thieves cannot create impersonating identities capable of executing the privileged authentication, privacy and attestation operations of the owner. Relying parties should be liable when they fail to conduct proof-of-private-key-possession tests before identity use.

Building Blocks



LinkedIn: Colleagues Attest to Skill Sets
Authorities and Known-Persons Attest to Identities

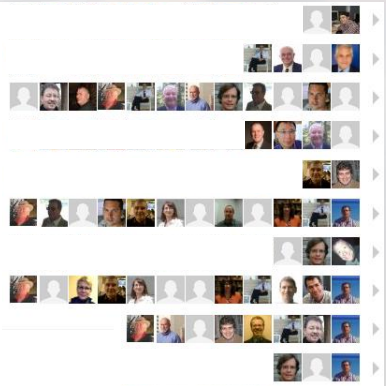
Cryptographic + Visual Identity Binding

(cannot be repudiated)

Owner's Identities

Multiple Attesting Identities

Birth and Baptismal Certs
Citizenship, Passport, Visas
Degrees, Training, Jobs, Skills
Work Authorization, Residency
Health Accounts and Insurance
Business Cards, Prof Credentials
Credit Reports
Banking, Finance, Credit Accts
Social Clubs, Prof. Membership
Drivers License, Endorsements



Q & A

http://www.betterthanyourwallet.com

Other Capabilities that should be Supported

- ✓ Employ a Trusted Execution Environment (trust zone, TPM):
  - ❑ Isolate identity processing and storage from malware/hacking
- ✓ Incorporate Identity Dashboard with Controls:
  - ❑ Identity and authentication assurances to fit transactional risks
  - ❑ Proof-of-possession challenges by either or both parties
  - ❑ Remote re-authentication on demand to verify user persistence
  - ❑ Request multiple authentication factors to elevate assurances
- ✓ Templates to specify a range of electronic identities:

Drivers Licenses	Degrees and Diplomas
Credit Cards	Business Cards
Debit/Banking Cards	Employee IDs
Health Insurance Cards	Social Club IDs
Birth Certificates	Certified True Copies of Physical IDs
Citizenship Cards	Pseudo-Anonymous IDs
Passports	Anonymous IDs (Blogging Canine)

Software Security Engineering (1)

- ✓ Specify unambiguous requirements:
  - ❑ Bind user to their device – a prerequisite to all other identity actions
  - ❑ Specify multiple key-pairs for each identity:
    - For each distinct purpose (e.g. authentication, encryption and attestation)
    - For multiple users accessing the same shared service (e.g. bank account)
  - ❑ Hold parties accountable for actions by capturing their "intent" (eSign Act):
    - Log transactions and/or
    - Attach intent to related object (identity or document)
    - Identities used, date-time, action (purpose, authorization, commitment)
  - ❑ Enable multiple attestations of the same identity to elevate assurances

Software Security Engineering (2)

- ✓ Make sound system and software design decisions:
  - ❑ Employ proven symmetric and asymmetric key libraries
  - ❑ Implement reliable escrow procedures saving/restoring identities and keys
  - ❑ Ensure that identities and keys can be revoked, expired, and updated independently
  - ❑ Protocols designed to prevent MITM attacks (e.g. OOB OTP exchange)
- ✓ Implement commensurate defect detection and prevention SW:
  - ❑ Ensure both end-points challenge the remote party when establishing a secure session
  - ❑ Use encryption to envelop authentication tokens
  - ❑ Inspect challenge-response protocol logic and tokens to prevent bypass

Identity Technologies Reviewed

1. Remote Access Passwords / PINs [P/P]
2. Federated Identity / Single-Sign-On [SSO]
3. Public Key Infrastructure + Client Certs [PKI]
4. Pretty Good Privacy + Client Certs [PGP]
5. Derived Credentials [DCRD]
6. Fast IDentity Online Authenticators [FIDO]

Password / PIN Based Identity [P/P]

- **Description:** Passwords and PINS are secrets known only to the user that are registered with remote services and used to gain access at logon time. The user is responsible for remembering and safeguarding their passwords/PINs; and services are responsible for safeguarding user passwords/PINs their enrolled personally identifying (private) information. Services are not obliged to encrypt the client-server channel (but should).
- **Identity Specification:** The relying service decides which private user info, if any, to enroll.
- **Identity Proofing:** The rigor applied to proof the user and the user's identifying information is determined by the relying service, and can range from zero to rigorous.
- **Identity Attestation:** No obligation to perform or record identity attestations (*e.g. when, who, type, rigor of identity proofing performed*).
- **Local Authentication:** Local user authentication is not required.
- **Remote Authentication:** Password/PIN is used to remotely authenticate the user.
- **Remote Channel Security:** The client-to-service connection may or may not be encrypted.
- **Strengths:** The Password/PIN scheme is a very simple remote authentication scheme.
- **Vulnerabilities:** The service's identity repository is vulnerable to large scale breeches revealing personally identifying information of the user, including credit-card information, and possibly user passwords/PINs, that could be used to create fraudulent physical and electronic credentials subsequently used to impersonate users and launch fraudulent transactions as if they were originated by the user.

Federated Identity / Single-Sign-On [SSO]

- **Description:** An identity framework consolidating identity-provisioning by establishing a service (or services) that enrolls users and their authentication data when registering, and subsequently authenticates them when they logon. Such SSO service nodes are integrated with relying servers and services by means of SAML-based protocols.
- **Identity Specification:** SSO service decides how much of user's private info is captured.
- **Identity Proofing:** SSO service determines rigor of identity proofing performed.
- **Identity Attestation:** No obligation to perform or record identity attestations.
- **Local Authentication:** Local authentication to a user device is not required.
- **Remote Authentication:** Password/PIN is typically used to remotely authenticate the user (FIDO authenticators are beginning proposed to authenticate users).
- **Remote Channel Security:** SSO solutions routinely encrypt the remote channels from clients to servers thereby protecting transmitted passwords/PINs/hashes/biometrics.
- **Strengths:** Number of user passwords/PINs needing to be remembered is reduced.
- **Vulnerabilities:** However, SSO does not specify identity assurance processes or schemes aimed specifically at reducing the risk of passwords/PINs and private user information being breached by a determined attacker.

Public Key Infrastructure: Client Certs [PKI]

Leverages public/private key crypto {PPC}

- **Description:** Public Key Infrastructure is an identity-provisioning technology that is ubiquitously available across the web targeting servers and services rather than users. PKI's "hierarchical trust model" employs X.509 standard digital certificates, public-private key encryption (RSA, EC), and symmetric key encryption.
- **Identity Specification:** Client certificates capture a limited amount of private info.
- **Identity Proofing:** PKI certificate authorities rarely perform meaningful identity proofing of users (servers and their certificates tend to be proofed to a higher standard).
- **Identity Attestation:** Authority weakly bound to signing key: signature can be repudiated.
- **Local Authentication:** Client software using PKI is not required to authenticate the user.
- **Private Keys:** Generated and retained by a central certificate authority.
- **Remote Authentication:** Authenticates private key possession using public key crypto.
- **Remote Channel Security:** PKI encrypts the client-server channel using available certs.
- **Strengths:** PKI can strongly bind a client holding the private key to the remote service.
- **Vulnerabilities:** There is some risk that the user's private key may be revealed to other parties during key distribution or by the CA. Weak 3rd party proofing reduces assurances to relying parties that originator impersonation has not taken place. Lack of prescribed local authentication reduces assurances that the personally identifying information is that of the owner and that their private key was used to secure the remote channel.

Pretty Good Privacy: Client Certs [PGP]

Leverages public/private key crypto {PPC}

- **Description:** Pretty Good Privacy is an open source identity-provisioning technology targeting peer-to-peer communications among PGP client modules. PGP implements a "web of trust" model and employs X.509 digital certificates and public-private key pairs. PGP creates client certs and associated key pairs, and exchanges certs with other users.
- **Identity Specification:** Client certs capture a limited amount of private user info.
- **Identity Proofing:** PGP users inspect and sign (attest) each other's client certificates.
- **Identity Attestation:** Attester weakly bound to signing key: signature can be repudiated.
- **Local Authentication:** PGP software does not mandate local user authentication.
- **Private Keys:** PGP clients do not release the private keys they generate to other parties.
- **Remote Authentication:** PGP implements peer-to-peer authentication using public key crypto. PGP assumes client-server channels have been secured by other means.
- **Remote Channel Security:** Peer-to-peer privacy to achieved using public key crypto. .
- **Strengths:** PGP strongly binds collaborating users by way of PGP client software keys.
- **Vulnerabilities:** When compared to PKI, PGP significantly reduces privacy and originator authentication risks because users' private keys are not revealed to others. However, like PKI, ad hoc 3rd party proofing coupled with lack of a prescribed local authentication mechanism, reduce assurances that the personally identifying information of a given certificate, and the associated private key, are those of the PGP client owner.

Derived Credentials [DCR]

Personal Identity Verification (PIV), Common Access Card (CAC), public/private key crypto {PPC}

- **Description:** The Federal Government plans to integrate PIV/CAC cards with personal computers and mobile devices. PIV/CAC cards are PIN and chip smart cards issued to government employees and contractors bearing a user photo and containing personally identifying information, three X.509 digital certificates, and public/private key pairs. At this stage it appears that this solution targets client-server usage only.
- **Identity Specification:** Contain user photo and predetermined identifying information.
- **Identity Proofing:** Designated authority proofs and installs user info, PIN and keys.
- **Identity Attestation:** Physical markings and embedded certificate(s) of authority.
- **Local Authentication:** The user is required to enter the PIN on each use of the card.
- **Private Keys:** Generated and retained a central authority (PIV/CAC issuer).
- **Remote Authentication:** "Derived" keys are to be used authenticate the originating card.
- **Remote Channel Security:** "Derived" keys are to be used to encrypt transactions.
- **Strengths:** Embedded personal digital certs coupled with PIN access enables strong authentication of the originating user as well as strong encryption of the collaboration channel. PIV/CAC cards are FIPS 201 and DoD compliant tamper-resistant devices.
- **Vulnerabilities:** Given private keys of the user are retained in a central repository, this solution is vulnerable to server-side breaches. Some have expressed concerns that the derived keys could be compromised within user devices.

Fast Identity Online [FIDO]

Leverages public/private key crypto {PPC}

- **Description:** Designed for client-server applications, FIDO devices authenticate the bearer by one or more factors (possession, knowledge and/or a biometric). Upon initial password logon to an existing service, the FIDO authenticator generates a public-private key pair registering them with the service, subsequently replacing password login with FIDO's public-private key authentication scheme. Note: peer-to-peer not supported.
- **Identity Specification:** FIDO does not capture personally identifying info of the holder.
- **Identity Proofing:** FIDO devices do not support identity proofing of users.
- **Identity Attestation:** FIDO does not attest the user and their identifying information.
- **Local Authentication:** A FIDO device is locally bound to the holder by multiple factors.
- **Private Keys:** FIDO devices do not reveal the private keys they generate to other parties.
- **Remote Authentication:** Public/private crypto authenticates originating FIDO devices.
- **Remote Channel Security:** Public/private crypto encrypts FIDO client-server channel.
- **Strengths:** Private keys being generated and safeguarded within a FIDO authenticator mitigates certain private key compromises. FIDO biometric-based authenticators reduce the need to remember and safeguard multiple PINs/passwords. Being hardware based, FIDO authenticators are more tamper-resistant than software based solutions.
- **Vulnerabilities:** FIDO does not capture, proof or attest to the identity of the user bearing the authenticator. Authenticating only the private keys held by the device, remote parties do not receive explicit assurances as to the FIDO device holder's identity.