



Next generation NSTIC
compliant digital identity

Steve Kirsch
Founder & CTO
stk@oneid.com

FICAM approved IdP isn't good enough

- Top CIOs: Solving ICAM is #1 for 2012
- OpenID:
 - Top providers (Google, PayPal) aren't allowing login w/anyone else's OpenID
 - Embarrassing security holes (see wikipedia)
 - IdP centric so not E2E secure
 - Weak protocol + weak IdPs = very weak
 - UX is confusing: NASCAR page of providers
 - Auth only; no agreement beyond that
- SAML is worse

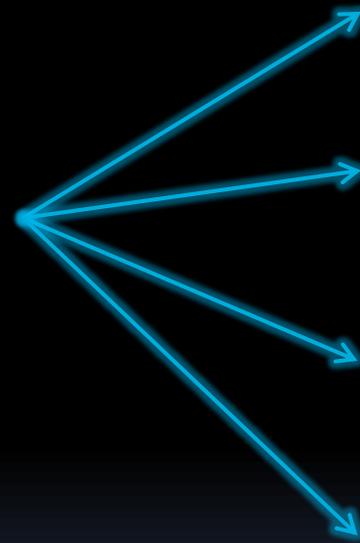
What is OneID?

- High assurance, **general purpose** digital identity ecosystem. Eliminates all use of shared secrets including usernames and passwords
- Designed from scratch to **exceed** all NSTIC requirements:
 - Easy to use; easy to deploy; **uses existing devices**
 - Security “on demand”: multi-factor **and OOB to LOA₄**
 - User centric, **preserves privacy**
 - Multi-provider w/identical spec (VISA, but for identity)
- 20 people... \$7M funding... Public launch October 2012... **> 375 RPs** today (pre-launch)

What does OneID do today?

- Authentication (AuthN)
- Authorization (AuthZ)
- Digital claims storage and assertion
 - A framework to allow **ID proof just once** for all RPs
 - Allows proving w/privacy, e.g., “here is proof I am over 21 and here is an associated biometric to prove it is me” w/o disclosing DOB, name, identity.
- Secure attribute storage & sharing
- Secure information storage & sharing

OneID provides ONE digital identity for all uses



Websites

Enterprise Apps

Desktop, Mobile Apps

In-person; over phone

Convince your device URU

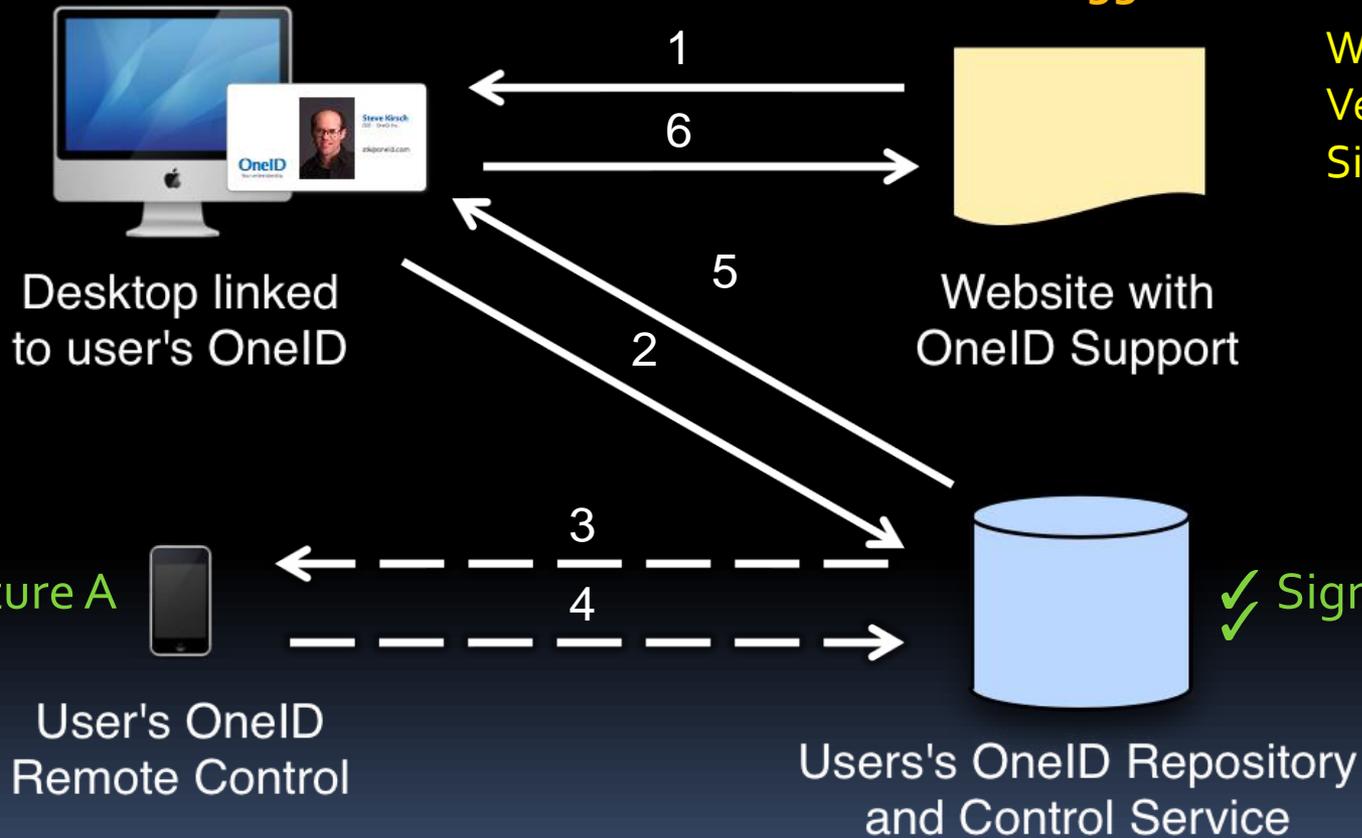
Your device digitally asserts your ID to everyone else using PK (with your express approval)

OneID Login Signature Flow

✓✓ Signature C

After verification,
user is logged in

Website
Verifies
Signatures



What's unique about OneID?

- **General purpose:** A single identity for web, desktop, enterprise apps
- **Guaranteed privacy:** Identity asserted/shared only if express consent
- **Mass adoption:** **Free**. Top e-tailers love it. People will already have it.
- Speeds up transactions, reduces friction, fraud
- User friendly: crypto management is hidden, 2-factor, OOB/PIN LoA
- NIST 800-63 **LOA4 capable:** Uses NSA Suite B crypto (ECC P-256).
Issue identity *then* adds certifications
- **"Have it your way"** LoA: $\max(\text{user}, \text{RP})$
- Six secrets are all distributed: user endpoint devices + cloud
- Secure: The architecture (*not operational policy*) guarantees **a mass breach is impossible** @ RP, IdP. Anyone can verify. Code is public.
- Reliable: **Works even if OneID down**

"This is exactly what the government needs"

OneID auth mimics real life



- “Hi. I’m Dr. Fred Smith. Here is my license. Here is my signature.”



- “Your signature matches and the license hasn’t been revoked.... OK, you’re authenticated.”

Issuance of physician credentials

- Login to mbc.ca.gov
- Click button "Add license cert to my OneID"
- mbc supplies CRL via rsync to (third party) verifiers used by RPs

Acceptance of physician credentials: simple!

- Doctor hits **Submit prescription** button in his EMR system to digitally sign transaction and include his license cert
- Everyone in the chain can verify:
 - EMR system → Surescripts → Pharmacy

Patients can be authenticated as well

- Using the same system
 - that they will already have and know how to use
- Easy 2-factor OOB authentication using mobile phone app
- Create identity w/2-factor OOB in < 2 minutes

Other

- Demo available:
 - adding a medical license
 - asserting it at a different RP
- Written material has IdP requirements checklist
- Open to collaborate on the design
 - Now is the best time