OneID Overview

# What is OneID?

OneID is a next-generation digital identity service designed for use by consumers as a more convenient and secure replacement for usernames and passwords.

Consumers log into their browser using OneID (using their preferred method of authentication). There are no usernames to remember. Passwords are optional. Once you’ve logged into OneID, users can sign into any OneID-enabled website just by clicking the OneID Sign In button on that site without further authentication (unless configured by the user or the site).

OneID is device-based. New devices must be pre-authorized using a one-time process that takes less than 10 seconds. Because of this, logins are easier, safer and more secure than any other method (including enterprise class secure two-factor methods such as SecurID, etc).

OneID doesn’t require any special hardware.

Several levels of assurance (LoA) are supported and can be set by the user or the website. LoA can be set on a per device, per website, and per transaction basis (e.g., based on dollar amount). OneID provides password, as well as 1 and 2-factor out-of-band authentication and authorization. More importantly, it does all this in a way that consumers can use and understand and with devices a user already has.

OneID works with all modern day browsers without a download.

The OneID service is free to users and to websites.

A consumer can set up a OneID account (and link it to his legacy account) at a participating OneID website in a few seconds without typing. The benefit for the site is that there is no OneID username or password for the user to remember so it is easy for a user to return to the site. A website can add OneID QuickFill to their site in less than an hour; no server-side changes are required. Adding OneID as an optional way to login to a site can be added in a few hours.

OneID uses end-to-end secure protocols: transactions are digitally signed on the requesting endpoints using 3 independent NSA Suite-B-compliant ECC signature keys, and are verified against 3 public keys unique to each relying party. This is all hidden from view of the consumers who never know they are using public key cryptography to secure their accounts.

OneID was architected from scratch to solve today’s problems with identity. Because the typical OneID consists of 8 independent digital secrets spread over three independent devices, standard attacks such as physical theft, phishing, malware, man-in-the-middle, man-in-the-browser, and key logging are ineffective. OneIDs are very difficult to breach and in the event a device is breached, the legitimate owner can easily disable the attacker without having to change a password or PIN. Even if a OneID user’s PIN and password were to become known by an attacker, an attacker cannot log in as that user. Unlike usernames and passwords, re-provisioning the public keys at websites is never necessary, even if an attacker learns all the crypto secrets and keys on all of the user’s devices.

# Where can I try this out myself?

Go to <http://support.oneid.com>. Click the login link in the upper right. You do not need to verify your email. Then logout (upper right link) and login again. You are logged in securely without a username or password and no one can log in as you.

# What does OneID do?

The key identity functions:

1. Authentication (e.g., login)
2. Authorization (e.g., purchases)
3. Information sharing (e.g., form fill)
4. Digital claims (e.g., proving I am over 21 without revealing my exact age)

# What are the key user benefits?

OneID provides users with greater:

1. Convenience (no username or password to remember)
2. Security (extensive controls on per device, per website, and per transaction basis; 5 different security levels including 2-factor out-of-band)
3. Privacy (sites don’t
4. Control

# Why do websites like it?

1. Less friction for login, form fill, and purchases; users can get the convenience of Amazon One-Click
2. Better security and privacy for users (happier users)
3. Better security and lower liability for the website (e.g., password database can’t be stolen since these are just public keys
4. Lower customer support costs (no more lost username or password)
5. Lower fraud (card not present)
6. Sites can avoid handling the credit card (no PCI liability)
7. Satisfies FFIEC 2-factor requirements
8. Users already know how to use it so minimal support costs
9. Users will already have it
10. Free for most websites

# What sites are committed to deploying OneID?

* One of world’s biggest countries (top 25)
* One of world’s largest credit card issuers (over 100M card holders)
* Large US airline
* A top 20 e-commerce site (launching OneID in November)
* [Four top e-commerce platform providers](http://www.oneid.com/about/news/ecommerce-partnerships)
* Early-adopter large bank
* Credit unions (November announcement)
* Several large PSPs reaching over 150M unique users
* A large US hospital chain (for patient login use)

# Who are the target relying parties for OneID?

Because OneID makes login easy, secure, and virtually eliminates typing, OneID is targeting:

1. Sites with repeat customers (e.g., e-commerce, membership organizations, donation sites)
2. Sites with infrequent customers who are likely not to remember username/password
3. Customer support areas (e.g., my.rackspace.com)
4. Sites with high security requirements (e.g., banks, hospital patient login)
5. Mobile websites
6. Mobile apps

Because a OneID can be created and the user doesn’t have to remember a username or password to log into his OneID account makes it very easy for a user to return to a site and log in successfully. This makes it more attractive for a site to issue a OneID than to issue a proprietary username and password. A [recent study showed that 38% of users would rather clean toilets than create yet another username and password](http://blog.sfgate.com/techchron/2012/08/23/rather-scrub-toilets-than-create-a-new-password-youre-not-alone/).

For existing sites, OneID is best offered as an optional way to log into a site, rather than a replacement.

For financial institutions, not only does OneID protect the customer, but it also protects the financial institution against a huge potential liability. For example, if an attacker acquires a traditional username/password file, they can drain accounts. With OneID, that can’t happen because there is no “password” file. It is simply a list of public keys.

# Who needs OneID and why?

Consumers need OneID because multiple usernames and password are both unmanageable and unsafe.

Social network logins would appear to solve the password proliferation problem, but introduce a new set of issues:

1. logging in with a social network (such as facebook) is unsafe (e.g., 600,000 compromised accounts on Facebook each day),
2. if your social network login is hacked (which is easy with a simple keystroke logger or phishing attack), all of your accounts are compromised
3. it isn’t private (Facebook knows your attributes and also when and where you’ve logged in), and
4. invariably you end up sharing information you never intended to share (e.g., if you log into Quora, you’ll be following all your friends even though you never asked to do this)
5. a bug or break-in at facebook can allow other people to pose as you or log in as you

Websites need OneID because it makes it easier and safer for users to log into sites and complete transactions. In particular, OneID reduces friction for e-commerce transactions.

More importantly, the world needs OneID because the current system is broken: it is unsafe and unmanageable. The biggest cause of the lack of security is the use of shared secrets. OneID eliminates the use of shared secrets. But OneID does much more than that. There are more than 40 innovations that OneID put together to create the world’s most advanced and most trustable third party identity service.

# What are some of the unique features of OneID?

1. Designed from scratch to solve the problem plaguing traditional identity systems
2. There are no usernames. Passwords are optional. A PIN code is required if you want out-of-band security that requires a PIN.
3. We got rid of all of the shared secrets. OneID uses public key cryptography to log into websites and for all proofs. There are no shared secrets.
4. We use modern-day NSA Suite B approved cryptography (256 bit ECC).
5. No downloads are required. Works on most modern day browsers.
6. Your identity isn’t centralized. Asserting your identity requires use of secrets at your endpoint device(s) and your chosen OneID identity provider. Three different cryptographic private keys are required to assert your identity. These keys are distributed into 3 different places: a web browser, a mobile application, and a cloud repository of the your choosing.
7. New, simple, elegant protocols guarantee end-to-end security for authentication and authorization.
8. It is very difficult to compromise your OneID identity because secrets aren’t centralized and because there no shared secrets and because there are 8 completely independent secrets that must be discovered.
9. It eliminates the major liability of a password file breach (especially for a financial institution where accounts can be drained). This is because the “password file” is replaced by a list of public keys which can be disclosed without any impact on account security.
10. You can choose which identity provider you want to use and change your decision at any time.
11. Any changes in your identity provider, PIN, password, devices, device secrets, device or website or transaction security levels, attributes, etc. can be done without having to notify or modify data at any relying party.
12. OneID is device-centric. You authenticate to your device and then your devices assert your identity.
13. Compliant with the principles of NSTIC
14. Users can pick any password or PIN that they want. If you choose to define a password, it doesn’t need to conform to any rules because it is only to secure your device from family members or co-workers who have physical access to your computers and will only be allowed a few guesses before the device is disabled (not your identity). The PIN must be at least 4 characters (due to financial institution requirements).
15. If someone steals all your devices and learns all 6 of your OneID secrets, you only have to remove the compromised device and add it back. It is not necessary to change your password or PIN and your ability to login at any site is unaffected.
16. There are easily accessible hints for your password in case you forget. These are only shown on pre-authorized devices and are inaccessible to websites that you visit. PIN and password secrets are never given to the OneID servers, not even in hashed form. If you forget your password or PIN, your account is not recoverable.
17. Common attacks do not work including phishing, malware, physical theft, and man-in-the-middle websites.
18. Your identity can never be asserted without your express consent (it always requires participation of one of your devices).
19. Your identity provider knows nothing about you other than your email address.
20. Assurance levels can be set by the user or the relying party (RP) on a per device, per website, and per transaction basis
21. There is no NASCAR problem. The OneID Sign In button works on all sites regardless of which OneID identity provider you choose.

# Why is OneID important?

All of today’s consumer identity providers are based on usernames and passwords. These are all shared secrets and are at the heart of most of the major security breaches. This forces users to use unique passwords at each site which is not manageable by users. In addition, usernames and password are easily phished, keylogged, and subject to man-in-the-middle attacks such as fraudulent websites.

Secondly, virtually every identity provider has been broken into. So there is no trustable identity provider which forces each website to be its own identity provider. This is why users have to have hundreds of usernames and passwords: because nobody trusts anyone else (and for good reason!).

OneID solves many of the problems with today’s identity systems by combining several innovations into an elegant architecture that eliminates the use of shared secrets, and provides superior security, privacy, and user control. It is the first truly trustable third party identity provider. It is immune to the common forms of attack.

# How does OneID work?

When a user tries to log into a website, the website presents the user’s browser with a random number known as a nonce. This nonce also includes the callback URL of the site to prevent man-in-the-middle attacks. The nonce is signed with the user’s browser (using cryptographic secrets stored in HTML 5 local storage) and also by the user’s OneID repository provider. If the transaction requires a higher level of assurance (such as a change of address or a high value transaction that exceeds a pre-set limit), a push notification is sent to the OneID app on the user’s mobile device where a third digital signature is obtained using crypto secrets that are only stored in the mobile phone application. All signatures are NSA Suite B compliant 256 bit elliptic curve cryptography (ECC) signatures. The two or three signatures are returned to the relying party who verifies the signatures against the two or three public keys on file.

For attribute release to a relying party (RP), the RP requests the attributes, the browser proves its identity to the OneID repository, gets the encrypted attributes, decrypts them in memory, and sends this information to the RP over SSL. No unencrypted personally identifiable information is ever stored on the user’s devices or in the repository.

The browser code is in Javascript so that no downloads are required and all modern day browsers are supported including Safari on iOS devices.

There is a 20 page description of the cryptographic protocols used by OneID available upon request to qualified parties. The security of OneID is based on the security of ECC and not in the secrecy of the protocols.

# How secure is OneID?

OneID isn’t foolproof. The goal was to make identity at least two orders of magnitude more secure than today without creating a system that was too hard for people to use.

There are 8 independent “secrets” associated with a typical OneID identity and they are distributed across three different computers, two of which are very difficult to break into.

If an attacker can gain physical possession of your two classes of devices and also learn your password (if any) and PIN code, they can control your identity. But that is very difficult to pull off in practice and even if it happens, it can be easily stopped and the user doesn’t even have to change his username (since there isn’t one), password (since there usually isn’t one), or PIN to do that. So the bottom line is that even if someone learns all the secrets used on all your devices, they can be easily stopped and none of the RP sites need to be notified since none of the public keys used on any RP site need to be changed.

# How is OneID different from password managers?

OneID is not a password manager.

OneID never sends usernames or passwords to a website. Websites that support OneID always use the OneID challenge-response authentication protocol using public key cryptography. So secrets like usernames and password never leave the device that they are typed into. They are instead combined with a local salt to generate an asymmetric signing key used for signing cryptographic challenges. All this magic is kept invisible to users.

# How does OneID preserve privacy?

Each website is given a unique set of public keys for each user. So if “Joe” logs into 10 different websites, he will use different private key sets for each website.

In addition, the website can never know where the user’s identity is stored since it only interacts with the user’s browser. Similarly, the user’s cloud identity repository never knows what websites the user went to because it only interacts with the user’s browser.

# Do I need a phone?

The first release of OneID requires the user to have an iOS device or Android mobile phone. The next release of OneID will eliminate that constraint so that OneID can be used by all users who have a web browser.

# What if I lose a device?

You can enable/disable that device from any of your OneID devices at any time. A user who steals your devices will not be able to perform any high value transactions above a certain limit (that you specify) without knowing your PIN code.

# Can I define a password?

Yes, you can add or remove a password to your OneID account at any time. You can use any password you like and you can set a password hint which will be shown to you upon request when you are prompted for a password. These two features make it very hard to forget your password.

Passwords are useful if you share a device or are worried about your device being stolen and being used to complete a “low value” transaction.

High value transactions are normally protected by an “out-of-band” authorization (on your OneID mobile app) and a PIN code (4 digits or more).

Unlike today’s systems, in OneID your PIN and password are not shared secrets. These values are combined with a salt on the local device to create a signature key that signs a challenge from your identity provider. So the PIN and password secrets are never shared with any third party in any form (including hashed form). If anyone breaks into the cloud identity repository, they cannot pose as you.

# How does OneID compare with the alternatives?

Our biggest competitor is really a website’s existing identity system (the “Proprietary IdP case). Here’s how OneID stacks up:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Feature** | **OneID** | **Proprietary IdP** | **Facebook Connect** | **OpenID provider** |
| Login to IdP without username/password | Yes | No | No | No |
| Keeps your info private | Yes | No | No | No |
| Identity can’t be phished | Yes | No | No | No |
| Support form-fill on third party websites | Yes | No | No | No |
| Support one-click checkout on third party websites | Yes | No | No | No |
| Support multiple attribute sets for form fill | Yes | No  | No | No |
| Support 2-factor out-of-band trans | Yes | No  | No | No |
| Selectively disable a device | Yes | No | Yes | No |
| Change LoA required to login to a device | Yes | No | No | No |
| Set security on a per website basis | Yes | No | No | No |
| Set security based on dollar amount of transaction | Yes | No | No | No |

# How does OneID compare with 2-factor solutions like Authentify, Phone Factor, etc.?

OneID is a complete identity solution, not a 2nd factor of authentication.

These 2 factor authentication point solutions work fine when all the websites you use agree on the same two factor method. They do nothing to end username and password proliferation. That problem is still untouched.

And if you lose your out-of-band device? No problem! Just re-provision at 352 different websites!

Basically, 2 factor is a band-aid on a fundamentally flawed system.

# People are saying about OneID

Here are some quotes from corporate CIOs, identity architects, security bloggers, and CISOs, but typically their company doesn’t allow use of their names for official endorsements:

“We believe OneID will attract the most forward-thinking businesses to offer a more secure alternative to the way we sign in to sites and share personal information.”

-- [Vinod Khosla](http://www.khoslaventures.com/people_vk.html), General Partner, Khosla Ventures

“I believe OneID will be one of the most significant platforms to be built in the next 10 years”

 -- [Jonathan Heiliger](http://www.northbridge.com/team/jonathan-heiliger), General Partner, North Bridge Venture Partners

“OneID appears to have it. It appears to be built right ground-up to serve the cloud era, with the right underlying deep understanding of how these kinds of technologies should be implemented and deployed. This underlying understanding is pure innovation and is quite rare.”

 -- Avishi Ziv, Security and IAM/IdM veteran

“Who’s your competition?!? You guys are in a class by yourself.”

 -- Credit card company

“OneID is light years ahead of what anyone else is doing today.”

– Internet security blogger

“Nothing interesting has happened in authentication in a decade; this is the first really intriguing approach that we’ve seen.”

– CSO for a well known, early-adopter large bank

“This is exactly what the US government needs.”

– US government security architect (after a 3 hour briefing with the CIO of a large US government agency)

“This is the first system I’ve seen that can actually solve the problem”

– Former CIO of Priceline

“Fantastic idea”

– Former global CISO of Bank of America

“I consider the work you are doing great breakthrough work that the world truly needs.”

– Internet security expert

“OneID is an amazing solution.”

– Consensus feedback at one of America’s largest financial institutions

“We love your idea and the vision behind it.”

 – CTO of on-line retailer with over 20M on-line customers

“OneID seems to have a high potential to help solve the consumer authentication and identity theft problem in a usable way.”

– Bob Pinheiro, Kantara Initiative,
 Chair of the [Consumer Identity Workgroup](http://kantarainitiative.org/confluence/display/WGCI/Home)

“OneID is an all-out, world-changing infrastructure play…”

– [TechCrunch](http://techcrunch.com/2012/03/13/oneid-beta-launch/), March 13, 2012

Listed as #1 of “7 hot security companies to watch”

– [Network World](http://www.networkworld.com/news/2012/031312-security-companies-257182.html), March 13, 2012

The Foundation Global Cyber Security Center (GCSC.org), an independent research center based in Rome, analyzed various identity solutions and selected OneID as the most innovative and secure solution for identification and authentication. The Center compared OneID with other similar technologies, both commercial and open source.

Poste Italiane is testing OneID and they defined it a "disruptive technology" that could change the way Italians access eCommerce and any other Internet service. Poste Italiane is Italy’s largest company and they provide not only traditional postal services, but also banking, insurance, digital communications, eCommerce, logistics, mobile services, etc.

# About OneID

Founded: May, 2011

CEO: Alex Doll, is the former COO of PGP, a $100M security company

Founder: Silicon Valley serial entrepreneur Steve Kirsch

Financing: $7M

Investors: Khosla Ventures and North Bridge Venture Partners

Employees: 23 (as of September 20, 2012)