# Two-Factor Authentication for VPN Access

Trends in cloud computing, workforce mobility, and BYOD policies have introduced serious new vulnerabilities for enterprise networks. Every few weeks, we learn about a new instance of compromised security. Ranging from spam via social media sites to hacks into customer databases, such breaches can be costly on so many levels. Many recent breaches have one thing in common: an employee's password that was copied, discovered, or given away.

User passwords are great. We love them. But with an avalanche of popular sites and apps that require passwords, your employees' favorite secret words and numbers are all over the online universe—so they're far from secret. If the security of your network depends solely on a user password for VPN access, you could be leaving the doors wide open to your corporate secrets. Enter two-factor authentication.

Two-factor authentication adds a layer of security by combining two methods of authentication to establish the unambiguous identification of each user. With this additional protection, users have the convenience of anywhere-anytime access without exposing the network to unauthorized interlopers—a potential that can result in enormous costs associated with operational disruption, the loss of customer goodwill, and the loss of stakeholder trust.

Depending on your industry or your network architecture, two-factor authentication for VPN access may be mandatory. For example, compliance for health data (HIPAA) or for credit card data (PCI DSS) demands that your remote access VPN environment be protected with two-factor authentication.

Two-factor authentication makes use of (at least) two types of authenticating data, at least one from **two different** columns below.

| Something you KNOW | Something you HAVE | Something you ARE |
|---|---|---|
| Password/PIN | Token or calculator (with OTP) | Fingerprint |
| OTP | Phone (with OTP via SMS) | Face recognition |
| Certificate* | Machine/Hardware certificate | Iris recognition |
| | Smartcard | Keystroke dynamics |
| | TPM | |

*Might be considered "something you have" in some enterprise IT environments.

## “Something You KNOW” Factors

### Password/PIN

Passwords come in many shapes and sizes: passcodes, passkeys, PINs, etc. In all cases, we’re talking about a string of characters, usually chosen by the user, based on symmetric cryptography. The information may also be stored in the configuration of a VPN client. A password’s security is based on the complexity of the character combination and (even more) on its length. Most users choose passwords that are easy to remember, such as pet names, birth years, simple number strings—all of which are very easy to hack. More complex, longer passwords are safer, but may be harder for the user to remember (and harder to enter). A password is always vulnerable to a replay attack.

### OTP (One-time password)

As the name implies, an OTP is a password that’s only valid for one login and for a very short period of time. It may be generated every few seconds (for example, users receive a new OTP every 30 seconds on a token) or triggered by an event (such as when the user requests to log in). Some OTP solutions are web- or application-based—and provide only one factor of authentication. More common OTP solutions add external hardware, such as a token or a phone, to provide the second “something you have” factor of authentication. Compared with static passwords above, OTP solutions are not vulnerable to replay attacks.



### Certificate

A certificate is a public or private key that can include various data points, such as issuer, expiration date, and address—all information which is “known.” Primarily used for encryption for secure web browsing, certificates rely on a PKI (public key infrastructure) to create, manage, distribute, and revoke certificates. A PKI uses a pair of keys: a public key, plus a private key for authenticating the user. Because certificates are based on asymmetric (rather than symmetric) cryptography, they provide a higher level of security compared with passwords and OTPs.

## “Something You HAVE” Factors

### Token or calculator

Most OTP solutions work in conjunction with external hardware (a token, calculator, or phone), which receives or generates the OTP. Typically, tokens generate an OTP at a specific interval, while calculators generate an OTP only when information (such as a PIN or password) is entered. Token-based solutions use an authentication server that draws from a table containing an OTP for each token + time combination—opening up risks if the authentication server is compromised. This time-based method requires tight synchronization and additional hardware to support it.

With tokens and calculators, the device must be physically close at hand—not always convenient for the end user. Scalability can also be a concern: As your organization adds new users, you need to buy more devices, a nontrivial expense. In addition, tokens and calculators can be lost, stolen, or broken—requiring bothersome communication and replacement steps and adding to already steep implementation and maintenance overhead. To make matters worse, most tokens do not have replaceable batteries, so you’ll need to replace older devices before their batteries wear out, generally every few years.

### Phone

With a phone-based OTP solution, the OTP can be generated by an app on the phone or sent via text message. The authentication server generates an OTP on demand, which expires after a short interval, typically 30 seconds—removing the burden of synchronization, as with token-based solutions.

Since we can usually assume that every user has a smartphone, phone-based solutions remove the costs and complexity associated with dedicated hardware (tokens and calculators). If the phone breaks or is lost, the end user will likely replace it faster than the enterprise will replace a token or calculator. And since the user’s phone number probably won’t change, there’s no need to reconfigure the authentication server for the replaced device.

### Machine/Hardware certificate

These solutions rely on the fingerprint of a device, typically a computer, to bind a certificate to it—which means it cannot be used with any other device. The fingerprint of the hardware is “something you have,” which permits exclusive access to the certificate, “something you know.” There’s no risk if someone copies the certificate; it won’t work in connection with another hardware fingerprint. Some operating systems may not support machine/hardware certificates.

## Smartcard

To support “something you have,” a smartcard usually stores a certificate on an embedded integrated chip. Smartcard-based solutions are more secure than OTP solutions since certificates use asymmetric rather than symmetric (OTP) cryptography. As with dedicated OTP tokens and calculators, smartcards are subject to the headaches of rollout, maintenance, and replacement—plus the cost of the cards and card readers.

## TPM (Trusted Platform Module)

A TPM is a low-cost, low-performance, and low-capacity crypto chip that’s soldered onto the motherboard of a PC or other device—making implementation somewhat more challenging than other authentication methods. The chip has the same capabilities as the chip on a smartcard, but adds root-of-trust security. TPM provides the same security functionality as physical smartcards, but without the overhead associated with shipping and returning the cards. Currently, TPMs are only built into business-line hardware from certain suppliers, such as Dell and HP, and only supported by Windows; Mac systems and most smartphones and tablets do not support TPM. However, we expect TPM adoption to become more prevalent in the near future.

## “Something You ARE” Factors

### Fingerprint

The most common method of authentication via biometrics is the fingerprint. As more and more devices have built-in fingerprint authentication, users feel increasingly comfortable swiping or pressing a finger over a scanner—more so than with other scanning methods. However, compared with “something you know” and “something you have” factors, fingerprint authentication may result in false matches and false non-matches—so the user might get access without the correct fingerprint, or the user might be denied access even with the correct fingerprint.

### Face recognition

The face—or, more accurately, facial features—can be used to authenticate the user. With this approach, the user device must have a built-in, high-resolution camera and face recognition software. Otherwise, a camera/scanner peripheral will need to be attached, adding inconvenience for the user and adding cost for the enterprise. Successful authentication may depend on lighting conditions and the angle at which the user is facing the camera. Depending on the quality of the camera and sophistication of the face recognition software, false matches and false non-matches are fairly common issues.

### Iris recognition

The characteristics and pattern of the iris can also be used to authenticate the user. This method requires a very high-resolution camera and specialized scanner software—typically not available on most user devices. Iris recognition presents the same issues as face recognition, including the possibility of false matches and false non-matches and the importance of perfect lighting conditions and exact camera angle.

Authentication via face or iris recognition usually takes longer than fingerprint authentication. In addition, staring into a camera for a few seconds may make some users feel uncomfortable. However, in the future, we expect to see new devices that include higher-quality cameras and sophisticated scanning software that make face and/or iris recognition fast, easy, and secure.

### Keystroke dynamics

This behavioral biometric uses the manner and rhythm in which an individual types characters on a keyboard or keypad. The user must enter a few words or a specific sentence to authenticate—more time-consuming than other biometric authentication approaches, but the only one that doesn’t require a camera or scanner. Unfortunately, very few applications have interfaces that support authentication via keystroke dynamics.

## Putting Two Factors Together

There are many ways to combine “something” and “something” to firmly validate the identity of your users. Below are a few common examples to consider, ranging from sending an OTP via SMS to the user’s phone to combining certificates with smartcards or fingerprint scans.

### OTP + phone

When the user tries to connect to the VPN, the VPN solution sends a text message, or SMS, with an OTP for the current session. This solution only provides an OTP when necessary and doesn´t require any additional dedicated hardware. Specifically designed for remote access VPN users, NCP’s OTP + phone solution is included with the NCP Secure Enterprise Management (SEM). The OTP is randomly generated by the system at login, providing stronger authentication—in contrast with token- or calculator-based hardware solutions that draw from a table generated by an authentication server.

### Certificate + smartcard

The certificate (“something you know”) is stored on the smartcard, which the user inserts into a smartcard reader. Depending on your requirements, you can specify if a PIN is required along with the smartcard, adding a layer of security. Because this solution uses certificates, there´s no symmetric cryptography (as with passwords) involved—another security advantage. The initial purchase of the smartcards and smartcard readers, as well as the ongoing overhead of supporting the hardware, are among the disadvantages of this solution.

### Certificate + TPM (virtual smartcard)

The certificate (“something you know”) is stored on the TPM on a PC, the second factor of authentication (“something you have”). As with the certificate/smartcard combination, you can configure the TPM to require a PIN. As noted above, TPMs are not currently built into all devices and are not supported by all operating systems.

### Certificate + fingerprint

In this combination, the certificate can be unlocked using fingerprint-based authentication. The user swipes a finger over the scanner, which unlocks the certificate if it recognizes the fingerprint. No additional hardware is required—assuming a fingerprint scanner is built into the user’s device—and you have the security advantages of asymmetric cryptography.



Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

### OTP + calculator

The user needs to enter a PIN into the calculator. The calculator generates the OTP with which the user is authenticated. This solution only provides an OTP when needed, but also requires more user interaction than other OTP solutions.

### Common combinations at a glance

| Two-factor combination | Additional hardware? | 3rd party vendor? | Client-side simplicity | Admin-side simplicity | Comments |
|---|---|---|---|---|---|
| OTP + phone | no | no | ***** | ***** | Easy to use and easy to implement; no need for dedicated hardware |
| Certificate + smartcard | yes | yes | *** | ** | Requires PKI, smartcards, and smartcard readers |
| Certificate + TPM | no | yes, to manage the TPM | ***** | ** | Easy to use; requires third-party vendor; requires PKI; not available on all platforms |
| Certificate + fingerprint | no | no | ***** | *** | Security advantages of biometric method; requires PKI and fingerprint scanner |
| OTP + calculator | yes | yes | *** | *** | Broad support; requires more user interaction; requires hardware purchase and maintenance |

### Going overboard

It's possible to set up a two-factor authentication solution that's super-secure, but totally unacceptable for the end user. For example, a company may combine OTP, token, smartcard, and certificate. In this "solution," the user must carry a token, a smartcard, and a smartcard reader—requiring them to read the OTP on the token, enter the OTP, plug the smartcard into the reader, and enter the PIN for the smartcard. In the end, the process is so complex that users are likely to demand a simpler solution.

## Barriers to Adoption

While the need for two-factor authentication is well understood in the enterprise IT market, its adoption rate is still surprisingly low. What stands in the way of widespread adoption?

- The second factor of authentication provides another layer of security and—oftentimes—another layer of work.
- Some VPN clients, operating systems, software applications, and web applications (basically everything with a password) do not support two-factor authentication. Vendors might not code their applications or create interfaces required to authenticate users in a secure way.
- An enterprise's user directory—particularly in the case of legacy directory services or architectures that require SSO (single sign on)—may not support a two-factor authentication solution.
- Most two-factor authentication solutions require the user to have specialized hardware, which IT staff must purchase, ship, and maintain and which users can lose or break.
- The second factor—"something you have" or "something you are"—typically adds rollout and maintenance overhead.

## Balancing Robust Security with Simplicity

With so many choices and so many obstacles, where to start? We suggest you choose a two-factor authentication solution that's ready for the future and for the growth of your business—from a vendor who's in tune with the latest trends and technologies. Choose a solution that meets the following criteria.

### Fully integrated with VPN services

If your VPN vendor provides built-in two-factor authentication, you can be sure it's compatible with your VPN solution (both clients and VPN gateways). This integration will also save time and headaches, since you don´t need to deal with two different vendors—one for VPN and one for authentication—speeding up implementation and reducing helpdesk support costs.

### Easy to implement

Make sure the two-factor solution you choose is easy to implement and does not introduce new admin challenges. For example, instead of shipping tokens or smartcards, you can use existing hardware, such as phones, for the second factor of authentication.

## Easy to maintain

It's even more important that your two-factor authentication solution be trouble-free to maintain. Administrators often underestimate the increase of helpdesk calls that result from implementation of a complex two-factor authentication solution—whether due to cumbersome authentication steps or specialized hardware that users may break or lose.

## Scalable

Many two-factor authentication combinations work great in small environments. It´s no problem to ship tokens to 50 end users. But if you have 5,000 or 10,000 end users, the purchase and shipping of "something you have" components or "something you are" scanners can challenge your IT budget. In addition, you'll want to make sure your two-factor authentication solution comes with central management, with automated updates, so it's easy for you to support the needs of your growing organization.

**For questions or to schedule a demo,**
**please contact NCP at 650.316.6273 or sales@ncp-e.com**

**About the Author**

Julian Weinberger, CISSP, is Director of Systems Engineering for NCP engineering. He has ten years of experience in the networking and security industry, as well as expertise in SSL-VPN, IPsec, PKI, and firewalls. Based in Mountain View, CA, Julian is responsible for developing IT network security solutions and business strategies for NCP. He also provides the company's key accounts with pre- and post-sales technical support for their remote access security solutions.

**About NCP engineering**

Since its inception in 1986, NCP engineering has delivered innovative software that allows enterprises to rethink their secure remote access and to overcome the complexities of creating, managing, and maintaining network access for their staff.

Headquartered in the San Francisco Bay Area, NCP serves 35,000+ customers worldwide throughout the healthcare, financial, education, and government markets, as well as many Fortune 500 companies. In addition, the company has established a network of national and regional technology, channel, and OEM partners to serve its customers.

For more information about NCP's remote access VPN solutions, visit www.ncp-e.com.
You can also reach us on our blog, VPN Haus, or on Twitter at @NCP_engineering.


Next Generation Network
Access Technology

www.ncp-e.com