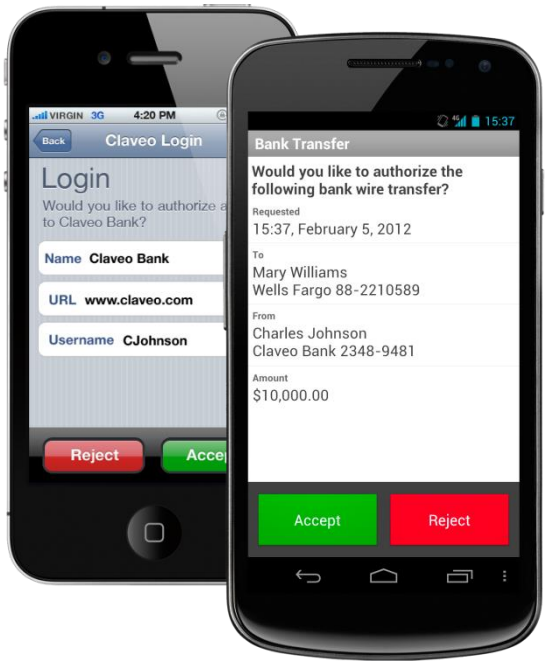
Claveo

# Two-Factor Authentication: What You Need to Know




***Not all two-factor authentication solutions are created equal. By asking the right questions, you can be confident in choosing among the many solutions available today.***

# Table of Contents

## Introduction to Two-Factor Authentication:

Over the past few years, the upward trend in advanced cyber security attacks has become a leading concern for businesses, governments, and even individuals. As we create, use, and store more information than ever before, passwords are no longer enough to prevent sophisticated hackers from compromising online accounts. In order to defend against this new generation of cyber-attacks, more and more organizations are turning to two-factor authentication.

What is two-factor authentication? Two-factor authentication (2FA) requires two of the three separate types of identity verification in order to access an online account or system:

1. Something the user knows (like a password or icon)
2. Something the user has (like a mobile device or token)
3. Something the user is (like a fingerprint or retinal scan)

By verifying two of these identification measures separately, online systems can be confident the users gaining access to critical information are really who they say they are. 2FA protects you from both internal and external threats:

**Internal Threats**

- Unsafe employee password routines
- Mobile employees on public networks
- Employee theft or sabotage

**External Threats**

- Stolen cookies or login credentials
- Phishing attacks
- Key loggers
- Trojans
- Malware and other threats

If your business handles any of the following items or must comply with any of the following regulations, you need to consider two-factor authentication:

*Sensitive user data*
*Trade secrets*
*Financial statements*
*Financial transactions*
*HIPAA*
*FFIEC*
*Strategic outlines*
*Employee records*
*Cloud infrastructure*
*PCI Data Security Standards*
*European Data Privacy Directive*
*Other proprietary information*

Not all 2FA solutions are created equal. This guide was created to serve as a tool for evaluating the various solutions available and to help you see why Claveo is the only second-factor solution for your organization.

## Security Question Checklist:

To confirm the second-factor authentication (2FA) vendor you are considering offers a truly secure solution, below are the ***three simple questions*** you need to ask. If a potential vendor ***cannot answer "Yes" to all*** of these questions, their solution is using outdated, insecure technology. Your security will be at risk – it's as simple as that.

### Questions for Potential Vendors:

1. Can you confirm that your servers neither ***see*** nor ***store*** any secret or personally-identifying information (PII) of users for ***any*** period of time?

2. Does your solution offer a tokenless ***and*** code-free user-experience? In other words, do you offer a solution that does not require users to carry around a physical token or type in additional one-time passwords?

3. If a user's primary credentials are stolen ***and*** your server is breached, are my users' accounts and my online system still protected? (In 2011, a single attack of this type exposed 40 million employee accounts with access to sensitive corporate networks)

### Claveo's Answers:

1. **Yes**. Claveo stores no private information and encrypts ***all*** transaction details as they pass through our server or integrated application. These details can only be seen on the mobile device during authorizations. This ensures that a breach of the Claveo system can never result in a fraudulent authorization.

2. **Yes**. Claveo delivers a convenient, token-free and code-free user-experience, without the need for expensive and frustrating additional hardware. Besides being difficult to replace if lost or broken and forcing users to type in cumbersome one-time passwords, physical tokens require you to trust a third party, who stores your users' secret information and may put you at risk (see question #1 above). Claveo puts security in your users' pockets with the mobile device they already carry everywhere.

3. **Yes**. Claveo protects your users no matter what. If an attacker steals a user's primary credentials and breaches our server, the attacker still needs that user's mobile device to make a fraudulent authorization. This eliminates the threat of system-wide breaches and makes cyber-attacks on Claveo users infeasible.

***When assessing 2FA solutions, remember to ask the three simple questions listed above.***

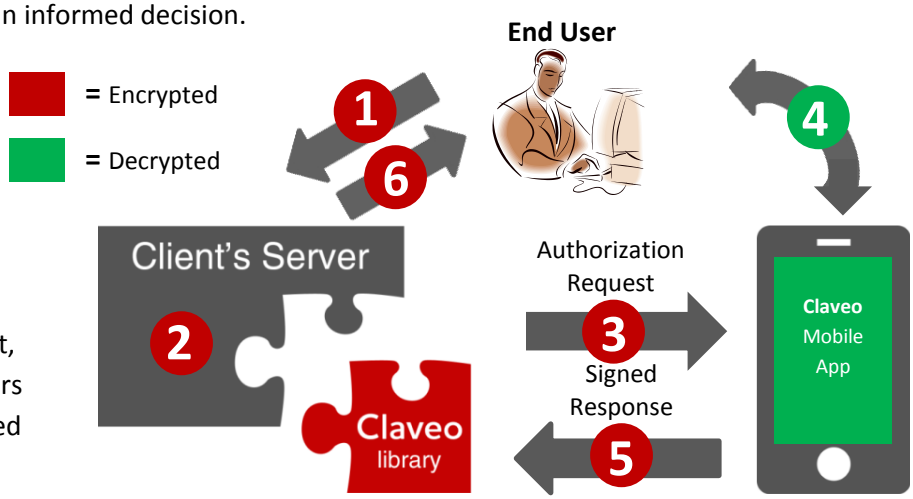
***If you hear a "No", you can't say "Yes".***

## Quality of Security:

Security is the chief concern of any authentication solution. When evaluating the quality of a solution's security, there are several factors to account for. It is vital that you become familiar with the components of authentication security in order to make an informed decision.

**General Criteria**

- End-to-end SSL encryption
- Out-of-band authentication
- Public key infrastructure (PKI)
- No secret information stored on "trusted" third party systems
- Hosted across multiple, redundant, highly-available secure data centers
- Management team with recognized expertise in cryptography




**Common Weaknesses**

- Use of split-key encryption
- Store information on "trusted" third party system
- Use of time-based rolling codes or one-time passwords
- Only protect from specific types of Man-in-the-Middle (MITM) attacks
- State that even if the server is compromised, your users remain protected because they still have their primary credentials. ***But aren't you considering 2FA because passwords are not secure?***
- Claim to never gather any personal information about users, but see it temporarily

**The Claveo Difference**

- Claveo neither sees ***nor*** stores any of your users' secret information. These details can only be seen on their mobile device during authorizations. This ensures that a breach of the Claveo server can never result in a fraudulent authorization.
- Claveo's tokenless solution guarantees that in addition to Claveo not seeing nor storing any private information, there is no "trusted" third party viewing or storing sensitive information either.
- Claveo employs public key infrastructure in the form of RSA 4096-bit security, protecting your users from ***all*** types of Man-in-the-Middle attacks.
- If an attacker somehow steals your primary credentials and breaches our server, the attacker still needs your physical mobile device to make a fraudulent authorization. In addition, mobile devices and the Claveo application both offer PIN options – creating up to ***five layers of security*** for your users.
- Claveo's team lives on the frontier of the cryptography industry. With extensive experience in cryptography and strong ties to leading research universities and security companies, our team's unique insight provides evolving and innovative solutions.

## Ease of Use:

Nobody wants an authentication solution that end-users find frustrating, time-consuming, or difficult to learn how to use – no matter how secure it is. The ideal solution should be easy, quick, and complimentary to your users' productivity or experience. When choosing a solution, prioritize its value to users and minimize overhead.

**General Criteria**

- Learning curve and necessary training
- Time spent per authorization and time granted to complete each authorization
- Effort and number of steps required per authorization
- Installation and enrollment procedures (time required and self-installation vs. admin-based)
- User adoption and sentiment
- Additional tokens or devices required to manage
- Functionality on all types of mobile devices
- User preferences
- Deactivation process


**Common Weaknesses**

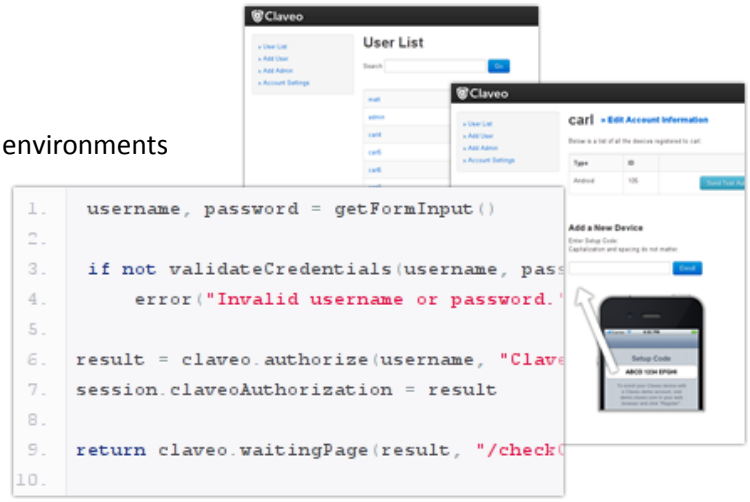
- Substantial installation time and effort required
- Time-based rolling codes pit users in an ongoing battle against the clock
- Additional hardware tokens to manage
- Steep learning curve preventing user adoption
- Substantial time and effort needed per authorization reduces productivity
- New installations needed per mobile device used
- No user preferences
- Complex device deactivation processes

**The Claveo Difference**

- Claveo's one-touch user interface requires little to no training at all – just a touch.
- By using public key infrastructure in place of time-base rolling codes, users can put races against the clock behind them. Claveo offers customized authorization expiration policies to better integrate with your standard IT practices.
- Users can self-enroll all types and as many mobile devices to an account as needed in minutes. Register your phone and tablet in less than 5 minutes!
- Claveo allows one device to authorize as many applications as needed. Use the same Claveo application on your phone to authorize logins for network appliances, VPNs, transactions, and more.
- Claveo offers users an extra security preference by offering the option of another security layer in the form of a PIN.
- With Claveo, all devices can be remotely deactivated with one click.

## Ease of Integration and Administration:

One of the biggest reasons organizations avoid 2FA is the frustration the integration and administration processes can cause IT departments. However, not all solutions are painful to implement. While the IT department may not have the final decision on which solution an organization chooses, they certainly are the ones who will understand its capabilities and spend the most time working with it. It is important to find a solution they trust and are excited to use.




**General Criteria**

- Documentation and support
- Integration with various existing platforms and environments
- Ease of adding and removing users
- Administration interface
- Extent of user training
- Scalability
- Automated self-service user options
- Lost or stolen device processes

**Common Weaknesses**

- Installation requires both hardware and software
- Requires constant updates and maintenance by IT staff
- Difficult and inflexible admin interface
- Requires admin attention for every user installation or removal
- IT department must spend extensive periods training users
- Complex device replacement processes (especially when hardware tokens are involved)
- IT security must write their own integration software

**The Claveo Difference**

- Installing Claveo can be completed in minutes, not months. In fact, implementation for most authorization applications (e.g. VPNs, customer portals, network appliances, etc.) can be finished and tested in hours. Once installed, Claveo's maintenance and update schedule is minimal and predictable.
- Claveo was created with flexibility in mind. Implementation into any existing platform or access point is easy. Claveo provides libraries for all major languages and software platforms
- Claveo's administration interface is intuitive and customizable. Administrators can control and monitor users, as well as adjust preferences to IT's standard practices.
- Once installed, users can add additional devices or accounts without administrator overhead.
- Claveo's one-touch user interface requires little training. That means no time spent training users for the IT department.
- With Claveo, users are responsible for replacing lost devices, not the organization.

## Cost of Ownership:

When comparing 2FA solutions, it is crucial to account for installation fees, usage fees, support fees, hardware fees, and any extra hidden costs. Additionally, many solutions have varying revenue models that can be difficult to assess. While value to your organization should be your number one criteria when procuring a security solution, you need to be able to calculate your budget and your total cost.

**General Criteria**

- Cost of any hardware or software components
- Effect on productivity due to time commitments (of end-users and IT department)
- Support costs
- Revenue model (per installation, per user, etc.)
- Cost of adding additional users

**Common Weaknesses**

- Significant upfront hardware investment
- High internal costs not accounted for in purchase (time)
- Replacing hardware that is lost or stolen (including shipping)
- Extra charges for integration into multiple environments
- Decreases in productivity from training time or lost devices

**The Claveo Difference**

- With Claveo, there are zero hardware costs – upfront or replacement. Claveo provides a free application for existing mobile devices, and users are responsible for replacing their own lost devices.
- Claveo's user and admin interface is extremely simple and intuitive, requiring little training by either IT administrators or end users. This lets your users maximize time and productivity.
- Claveo lets you calculate your budget and total cost by offering customized and flexible pricing models to meet your business needs.
- Claveo charges no additional fees for implementation to multiple environments and applications. Claveo subscriptions come complete with expert support and communication.

## Comparing Types of Second-Factor Authentication:

To compare second-factor authentication offerings, it is important to recognize the different types of solutions in the marketplace. The most common types of 2FA systems include hardware tokens, smartcards, certificates, and mobile-based solutions. Below is a grid comparing all of the various solution types:

| | Claveo | Certificates | Hardware Tokens | Smartcards | Other Mobile-based |
|---|---|---|---|---|---|
| **Criteria** | | | | | |
| **Security** | ★★★★★ | ★★ | ★★★½ | ★★★★ | ★★★ |
| **Ease of Use** | ★★★★★ | ★★★ | ★ | ★★ | ★★★★ |
| **Ease of Integration and Admin** | ★★★★★ | ★★½ | ★½ | ★ | ★★★★ |
| **Cost of Ownership** | $ | $$$ | $$$$$ | $$$$ | $$ |
| **Total** | ★★★★★ | ★★ | ★★½ | ★★★ | ★★★½ |

## Conclusion:

When considering a second-factor authentication solution, the quality of the security is the number one criteria; however, nobody wants a security solution that is difficult to implement and use or one that is exceedingly expensive. Overall, there are four main criteria you must evaluate when considering a 2FA solution:

1. Quality of security
2. Ease of use
3. Ease of integration and administration
4. Cost of ownership

With various authentication solutions flooding the marketplace, even the savviest IT administrators can be misled into choosing an inadequate solution. Claveo blends the most secure mobile-based 2FA solution with a pain-free implementation process and a one-touch user interface, giving your entire organization the security, experience, and peace of mind it deserves at a price you can afford. ***Only Claveo offers the second-factor authentication solution that your organization's users, IT department, and management will fully embrace. If your organization is considering a 2FA solution, make sure you get it right the first time.***

***Get secured by Claveo.***

We would love to speak with you about your second-factor authentication needs! Take the next step and contact us today to learn how Claveo can integrate with your online system.

Peter Vrouvas
Director, Business Development
Phone: (805) 308-6505
Email: peter@claveo.com

Try our DEMO at http://demo.claveo.com/
Sign up for a free trial here http://claveo.com/signup
Visit our website at www.claveo.com