# What is 2FA. Types and standards

Two-Factor Authentication (2FA) is a security mechanism that strengthens authentication by requiring two different types of credentials to verify a user’s identity. These credentials generally fall into three categories:

1. **Something you know** – A password, PIN, or answer to a security question.
2. **Something you have** – A physical device like a phone, smart card, or a one-time passcode generator.
3. **Something you are** – Biometric characteristics such as a fingerprint, facial recognition, or iris scan.

**How 2FA Works**

When a user attempts to log into an account, the following process typically occurs:

1. **First Authentication (Password/PIN)**: The user enters their username and password, which is the first factor (something they know).
2. **Second Authentication (Code or Biometric)**: After the first step is completed, a second factor (something they have or are) is requested. This could be a code sent to their phone via SMS, an app-based token, a hardware key, or biometric verification.
3. **Access Granted**: Once the second factor is successfully verified, access is granted to the user.

**Types of 2FA**

**1. SMS-based 2FA:**

* **How it works**: After entering the password, a one-time passcode (OTP) is sent to the user's phone via SMS.
* **Pros**: Simple and widely adopted.
* **Cons**: Vulnerable to SIM-swapping and interception attacks.

**2. Time-based One-Time Password (TOTP):**

* **How it works**: Using a mobile app like Google Authenticator or Authy, the user generates a temporary passcode that changes every 30-60 seconds.
* **Pros**: More secure than SMS since it works offline.
* **Cons**: User needs access to their mobile app or token device.

**3. Push-based Authentication:**

* **How it works**: A push notification is sent to the user's smartphone, which they can approve or deny. Apps like Duo or Google Prompt use this method.
* **Pros**: Convenient, no need to enter codes.
* **Cons**: Requires internet access, depends on the security of the phone.

**4. Hardware Tokens:**

* **How it works**: A dedicated hardware device (like a YubiKey) generates codes or communicates via USB or NFC to authenticate.
* **Pros**: High security, immune to phishing and remote attacks.
* **Cons**: Requires physical possession, can be lost or damaged.

**5. Biometric Authentication:**

* **How it works**: Uses fingerprint scanners, facial recognition, iris scanning, or voice recognition as the second factor.
* **Pros**: Highly secure, convenient.
* **Cons**: Can be costly to implement, may have privacy concerns, some biometrics can be spoofed.

**Standards for 2FA**

**1. Time-based One-Time Password Algorithm (TOTP):**

* **Description**: Generates temporary passcodes based on the current time and a shared secret key. This is widely used in apps like Google Authenticator.
* **Standard**: Defined in RFC 6238.

**2. HMAC-based One-Time Password (HOTP):**

* **Description**: Generates one-time passwords based on a counter and a shared secret. The passcode remains valid until used.
* **Standard**: Defined in RFC 4226.

**3. FIDO U2F (Universal 2nd Factor):**

* **Description**: A standard created by the FIDO Alliance that supports hardware authentication tokens (like YubiKeys). It uses public-key cryptography for authentication.
* **Pros**: High security and phishing resistance.
* **Standard**: Supported by browsers and services like Google and Facebook.

**4. FIDO2 (WebAuthn + CTAP):**

* **Description**: An evolution of FIDO U2F that enables passwordless login. It uses public-key cryptography and is implemented via biometric devices, USB keys, or NFC.
* **Standard**: Supported in modern web browsers via WebAuthn (part of FIDO2).

**5. Public Key Infrastructure (PKI):**

* **Description**: Uses a pair of cryptographic keys (public and private) for authentication. Often used in government or enterprise environments for high-security systems.
* **Pros**: High level of security.
* **Cons**: Complex to manage and implement.

**Common 2FA Implementations**

* **Google 2-Step Verification**: Uses either SMS, a Google Authenticator app, or push-based authentication.
* **Microsoft Authenticator**: Works similarly, using TOTP codes or push notifications.
* **Duo Security**: Popular in corporate environments, uses push-based authentication, TOTP, and hardware keys.
* **Authy**: A TOTP app with cloud backup features, useful for multi-device usage.

# What happens if 2FA is compromised?

* **Alternatives**
  + **Multi-Factor Authentication (MFA):** This extends 2FA by adding another layer, such as biometrics (fingerprint or facial recognition) or a hardware key like a YubiKey. This makes it harder for attackers to bypass security measures.
  + **Account Recovery Options:** Systems often include account recovery through backup codes, security questions, or secondary email accounts. However, this can introduce additional security risks if not handled properly​
  + **Risk-Based Authentication:** This method assesses the context of a login attempt (location, device, behavior) to determine if additional authentication is necessary. If a login seems suspicious, the system might require extra verification
* **Fallbacks**
  + Many systems have backup methods for 2FA, such as using backup codes, recovery questions, or alternative second factors like email authentication. However, these fallback methods can reduce security, as they may be easier to compromise compared to 2FA.
* **Mitigations**
  + **Backup Authentication**: Ensure secure backup authentication methods, such as hardware tokens or authenticator apps, which work offline or independently of the 2FA server.
  + **Grace Periods**: Some systems provide a temporary grace period where users can log in without 2FA if the server is down, but this should be carefully managed to avoid security risks.

# Articles

* Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication
  + <https://talpykla.elaba.lt/elaba-fedora/objects/elaba:102885619/datastreams/MAIN/content>
  + Note: Magistrinis ktu darbas, atrodo ok for references
* Two-Factor Authentication Resilient to Server Compromise Using Mix-Bandwidth Devices
  + <https://www.researchgate.net/profile/Maliheh-Shirvanian/publication/269196930_Two-Factor_Authentication_Resilient_to_Server_Compromise_Using_Mix-Bandwidth_Devices/links/56bcf66208aed69599460988/Two-Factor-Authentication-Resilient-to-Server-Compromise-Using-Mix-Bandwidth-Devices.pdf>
  + Note: detailed paper about 2fa, good reference for security related topics of 2fa. Detailed description of 2fa types, used communication protocols, reasoning, also about attacks.  
    **Needs** more investigation.
* [**Trust, Privacy and Security in Digital Business**](https://link.springer.com/book/10.1007/978-3-030-86586-3) (book)
  + <https://link.springer.com/chapter/10.1007/978-3-030-86586-3_11>
  + Note: **MULTI-FACTOR** authentication
    - This method assesses the context of a login attempt (location, device, behavior) to determine if additional authentication is necessary. If a login seems suspicious, the system might require extra verification
    - **Turbūt artimiausias dalykas kurį radau apie 2fa alternatyvas**. Dar vienas abstrakcijos lygis siekiantis papildomai apsaugot duomenis, on-need basis.
* A Method of Risk Assessment for Multi-Factor Authentication
  + <https://koreascience.kr/article/JAKO201113753748218.pdf>
  + Note:
    - Types of authentication:
      * Proof-of-Knowledge (Something you know?)
      * Proof-of-Possession (Something you have?)
      * Proof-of-Characteristics (Something you are?) -physiologically or behaviorally (Fingerprints, Hand geometry, Facial image, Iris, Retina, DNA, voice, signature patterns)
    - Includes Technical requirements, descriptions of authentication levels, references to good terms and security standards.
      * E.g. NIST 800-63 Electronic Authentication Guideline
* A Usability Study of Five Two-Factor Authentication Methods
  + <https://www.usenix.org/conference/soups2019/presentation/reese>
  + Note:
    - **Actual 2FA alternative** is presented:
      * Pre-generated codes are often a backup 2FA authentication method in case the user is unable to access their primary 2FA method. Implementation is straightforward: the service provider generates a list of verification codes and has the user print or write the codes down
* Cybersecurity Revisited: Honeytokens meet Google Authenticator
  + <https://arxiv.org/abs/2112.08431>
  + <https://arxiv.org/pdf/2112.08431>
  + Authenticators Comparison
  + Honeywords – fake passwords to catch if Database is leaked.
    - When a honeyword is send by the login phase, there will be an alert that the password database
    - An additional layer of security.

## Backend literature:

* .NET Core 2fa setup documentation:
  + <https://learn.microsoft.com/en-us/aspnet/core/security/authentication/mfa?view=aspnetcore-8.0>
* Google authenticator in asp net mvc project:
  + <https://tudip.com/blog-post/how-to-integrate-google-authenticator-in-asp-net-mvc-project/>

# How server failures are handled by popular 2FA enterprise solutions

* Cisco DUO:
  + <https://help.duo.com/s/article/5352?language=en_US#:~:text=The%20fail%20mode%20determines%20whether,primary%20authentication%20source%20is%20unreachable.>
  + Wow, solution is:
    - [https://duo.com/docs/dag-windows#additional-settings](https://duo.com/docs/dag-windows%23additional-settings)
    - **Either Allow or Don’t allow** users to connect when DUO is unreachable.
      * “. If the fail mode is **safe**, users who successfully pass primary authentication may access the cloud application without completing two-factor authentication. If the fail mode is **secure** then DAG requires that all users perform 2FA. If the user's client browser or application is then able to contact Duo and complete two-factor authentication then users proceed to the application or to the DAG Launcher page. If the user's client also cannot contact Duo for 2FA, then the user cannot continue.”
* Okta:
  + [https://support.okta.com/help/s/article/What-should-i-do-if-Okta-goes-down?language=en\_US#:~:text=If%20our%20services%20were%20to,accessible%20through%20a%20direct%20link.](https://support.okta.com/help/s/article/What-should-i-do-if-Okta-goes-down?language=en_US%23:~:text=If%20our%20services%20were%20to,accessible%20through%20a%20direct%20link.)
  + Solution:
    - Access is disabled for users if server is down
      * Okta is built on an “Always On” architecture. You can always go to [https://status.okta.com/](https://trust.okta.com/) to see our high reliability metrics and to learn more about the reliability of our service.  
          
        If our services were to go down, you would not be able to log in to your Okta organization and access your applications via Single Sign-­‐On. However, some applications might still be accessible through a direct link.
* OneLogin:
  + Can’t find any info about how servers are down are being handled
  + Only thing is this status screenshot of uptime showing 99.85%  
    A screenshot of a computer screen

    Description automatically generated

# Current questions, problems

* Difficult to find actual 2fa alternative switch articles, apart from MFA

# Scientific literature urls:

* [*Akademinių institucijų virtualios bibliotekos*](http://www.elaba.lt/elaba-portal/paieska/ivb)
* [*BASE*](http://www.base-search.net/)
* [*Dimensions*](https://app.dimensions.ai/discover/publication)
* [*Directory of Open Access Journals*](http://www.doaj.org/) ([DOAJ](https://open.ktu.edu/mod/glossary/showentry.php?eid=65&displayformat=dictionary))
* [*Google Scholar*](https://scholar.google.lt/)
* [*Lietuvoje prenumeruojamos duomenų bazės*](http://www.lmba.lt/duomenu-bazes)
* [*Lietuvos akademinė elektroninė biblioteka*](http://www.lvb.lt/) *([eLABa](https://open.ktu.edu/mod/glossary/showentry.php?eid=71&displayformat=dictionary" \o "Santrumpos: eLABa))*
* [*Lituanistika*](http://www.lituanistikadb.lt/lt)
* [*OpenDOAR*](http://v2.sherpa.ac.uk/opendoar)