toothpic

YOUR SMARTPHONE IS YOUR SECURE KEY

Unlock its potential with camera sensor hardware

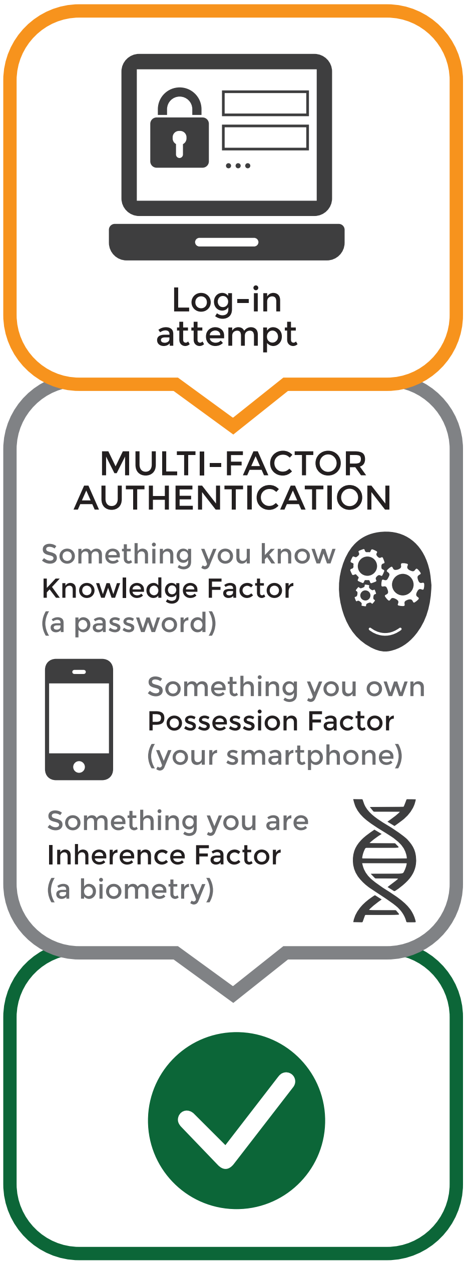
LEGACY **MULTI-FACTOR** AUTHENTICATION

Current authentication systems suffer from a trade-off between security and usability. It is well known that passwords, a 40 years old authentication method, are no longer sufficient to guarantee security in today's digital world due to inherent human limitations, whereby everybody owns dozens of digital identities and requirements like no-reuse or password complexity simply **cannot be met** [1].

Multi-factor authentication (MFA) systems complement the knowledge of a password (also known as knowledge factor) with:

- the verification of a biometric trait, or inherence factor (fingerprint, iris, vein pattern, behavioral authentication), which however has several problems like the confidentiality of biometric data and the **complexity of implementing** [2] it in consumer products, which may result in **issues** [3] and **security flaws** [4];

- the verification of a possession factor (e.g., the possession of a specific object, like a smartphone or a bank security token), currently implemented according to different security/usability trade-offs. Dedicated devices like USB tokens are secure but not very usable, do not scale well to every possible type of user or service, and are an **additional cost** [5] for service providers and/or users. Systems based on the user's smartphone are much more convenient, since everybody owns a smartphone, and can solve many usability problems. However, not all smartphone-based solutions are secure, even **widely used ones like sending a text code via SMS** [6].



Due to the above problems, MFA systems are not widely deployed nowadays, except when their use is mandatory. According to a **survey by Gemalto** [7] in 2017, out of 10000 consumers 56% declared to use the same password for multiple online services, and 41% refused to use an MFA system even when included in their social media platform. At the same time, 62% would consider the service provider responsible in the case of data breach and 70% would stop using their services in case of identity theft.

In a 2017 Gemalto survey of more than 10.000 consumer worldwide...

56%
said they use the same password for multiple online accounts

41%
declined to use two-factor authentication when offered the option for their social media accounts

62%
said that businesses are responsible for data security

70%
said they would part ways with a company if it experienced a data breach

Source: Gemalto survey

[1] https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-pw0rd

[2] https://nakedsecurity.sophos.com/2018/11/16/ai-generated-skeleton-keys-fool-fingerprint-scanners/

[3] https://www.theverge.com/2019/10/17/20919026/samsung-galaxy-s10-ultrasonic-fingerprint-sensor-security-flaw-screen-cover-protector

[4] https://www.androidcentral.com/how-secure-face-recognition-galaxy-s10

[5] http://symantec.postclickmarketing.com/Global/FileLib/White_Papers/Whitepaper_TFA_A_TCO_Viewpoint_(1000_users).pdf

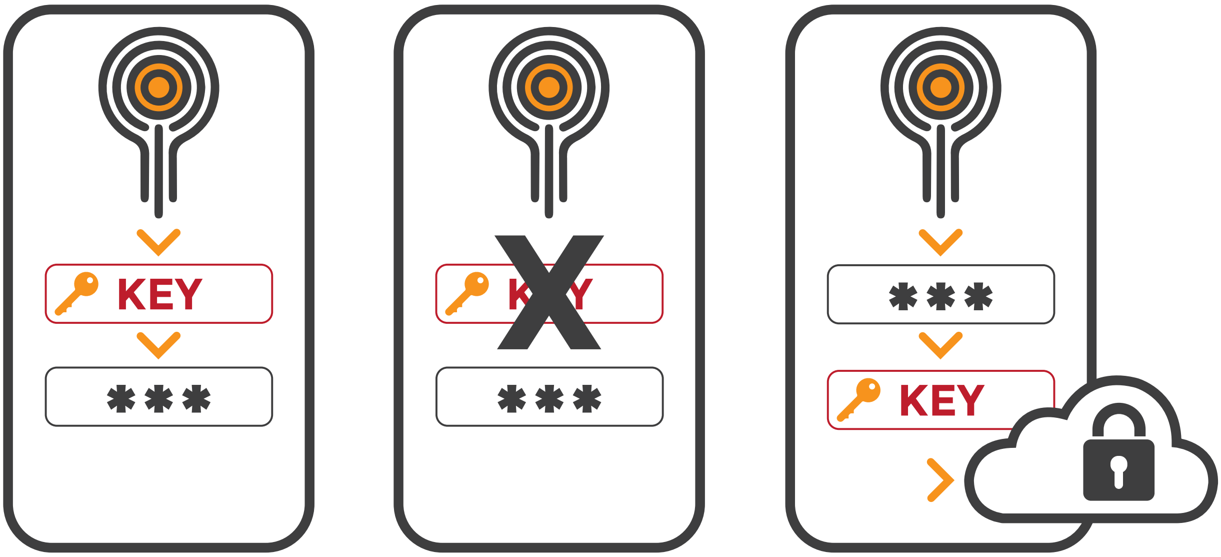
[6] https://techcrunch.com/2016/07/25/nist-declares-the-age-of-sms-based-2-factor-authentication-over/

[7] https://www.gemalto.com/press/pages/majority-of-consumers-would-stop-doing-business-with-companies-following-a-data-breach-finds-gemalto.aspx

TOOTHPIC
SOLUTION FOR **MFA**

ToothPic developed an innovative MFA technology overcoming the duality of security and usability. Our technology is able to recognize the user's smartphone through an invisible pattern of imperfections characterizing the millions of pixels of the camera sensor, which can be considered like a sort of unique hardware fingerprint. Since the pattern is due to unpredictable physical properties of the sensor silicon wafer, it is virtually impossible to produce two smartphones with the same camera fingerprint, thus resulting in a Physical Unclonable Function (PUF). The main advantage of ToothPic technology is that every user already owns a device that can be uniquely identified thanks to a random physical property. Differently from hardware serial codes (e.g., MAC addresses of network interfaces) this property cannot be decided by the manufacturer, so it cannot be cloned or masked. The adoption of this disruptive technology is extremely simple, since it does not modify user habits, it does not require new devices, companies implementing it do not have to invest money in new hardware or incur in additional costs. From the user's side, smartphone identification is just a click away, since all the procedure is completely automatic.

ToothPic deployed this innovative technology in an SDK for Android and iOS enabling the protection of standard asymmetric keys, making it ready to be used in every system based on standard asymmetric cryptography. Whenever a user needs to authenticate, sign a document, or authorize a transaction, he/she first provides a user credential (e.g., either a password, PIN, or biometric credential). Then, ToothPic SDK takes control of the camera for a few seconds and automatically acquires a few pictures to verify the camera fingerprint.



Thanks to ToothPic SDK, this disruptive technology can be easily integrated in any app or third party software to enable the verification of a possession factor. Possible applications are:

- Authentication systems, in which the user has to demonstrate possession of a specific device, even in passwordless modality. It is worth noting that our system satisfies recent regulations regarding **Strong Customer Authentication (SCA) and PSD2** [8] introduced in September 2019;
- Digital signature systems, in which a user's device becomes a digital signature device, without any additional hardware;
- Encrypted communication systems, in which encrypted messages and documents can be read only using the device with the right fingerprint;
- Crypto wallets, in which the cryptographic keys identifying users' wallets are protected by ToothPic technology, either when they are physically on the user's device or when they are managed by a **crypto exchange** [9].

Available as a mobile SDK for seamless integration Supports commonly-used EC cryptographic keys

Authentication

· Possession Factor Verification
· Strong Customer Authentication
· PSD2

Digital Signature

· Sign with your smartphone
· No additional device required

Encryption

· Trusted devices for company executives' documents and messages

Crypto Wallet

· Secure wallets for crypto users and exchanges

[8] https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_4961

[9] https://www.bloomberg.com/news/articles/2018-03-05/crypto-exchanges-raking-in-billions-emerge-as-kings-of-coins

BENEFITS OF TOOTHPIC **SOLUTION**

What are today considered as the best solutions for the verification of a possession factor follow an asymmetric cryptography paradigm, in which a user has a private key that should be kept safe and a corresponding public key shared with everyone.

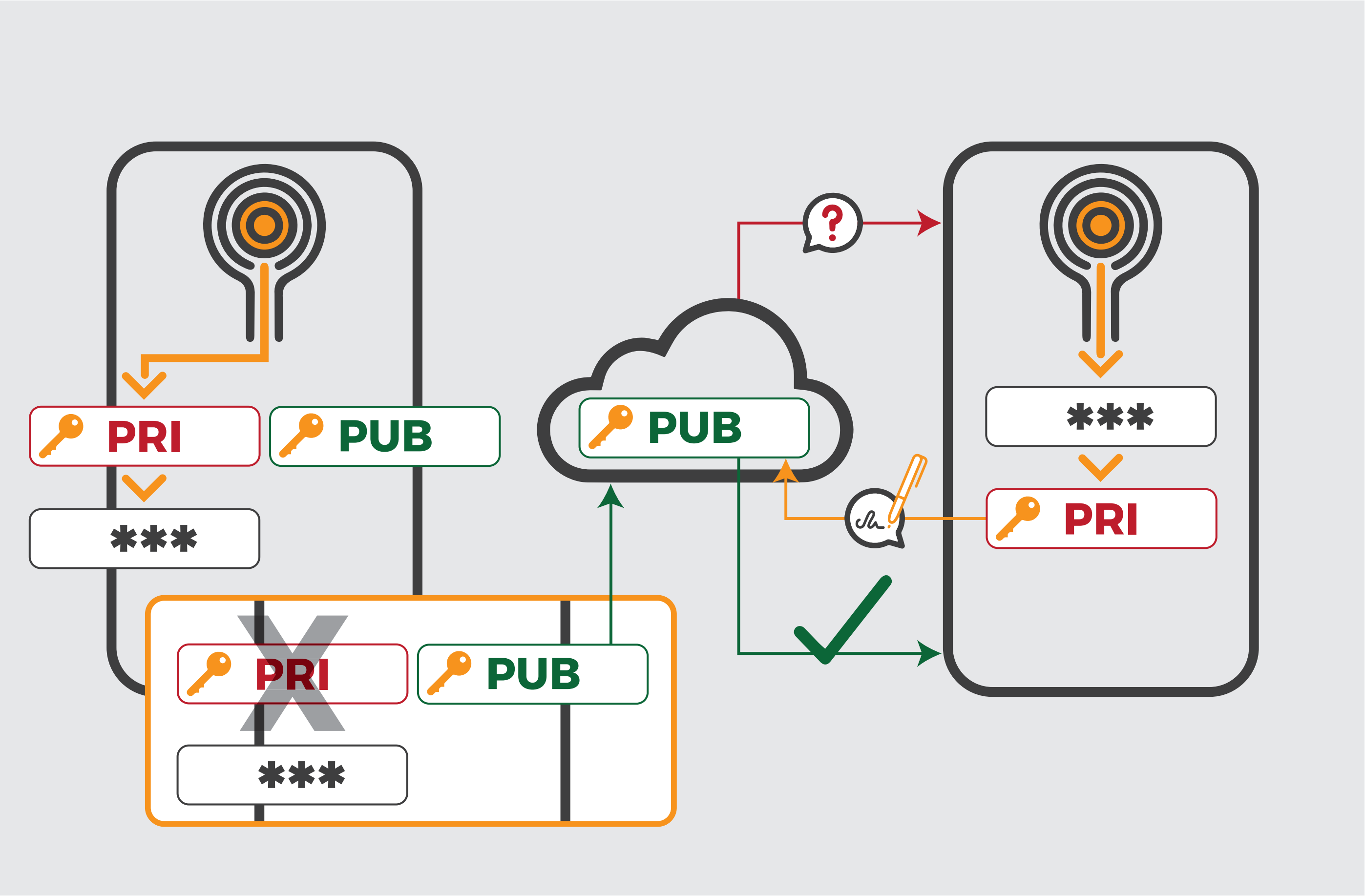
Only the authentication device is able to perform certain operations using the secret key. However, everybody can verify the result of those operations using the corresponding public key and confirm that they are indeed performed by the authorized device.

For user authentication a simple protocol can be established: the server sends a challenge message to the user, the user signs the message using the private key, the server verifies the signature with the user's public key. Since there is no shared secret between the server and users, there is no single point of failure at the server side. The only requirement is to protect each users' private key. Due to its enhanced security, this is the solution chosen by most recent authentication protocols like **FIDO** [10].

With ToothPic, the above solution can be implemented on generic devices, like a user's smartphone, in a much safer way:

- Differently from software based solutions, the secret key is never stored on the smartphone where it is exposed to malware. Whenever the secret key is needed, it is de-obfuscated on the fly using a fresh acquisition of the camera sensor fingerprint;
- Publicly available pictures from the same device, like those shared on social networks, cannot be used to de-obfuscate the secret key, since our technology computes the sensor fingerprint from features that are destroyed by image compression algorithms like JPEG;
- The use of an unpredictable physical feature of the hardware significantly reduces the attack surface. A user can lock the secret key by simply covering the lens of the camera (a common smartphone cover can do the trick). Even a malware taking full control of the device would not be able to remotely use the key in this setting;
- Users' credentials are not stored in a centralized service provider servers - representing a single point of failure exploitable by an attacker - but they are distributed on users' devices. Hence, an adversary willing to violate those credentials should target each single user device. The use of a system based on asymmetric cryptography facilitates the migration from an *on premises* architecture to the *cloud*, because service providers don't need to manage sensitive users credentials, but only their public keys.

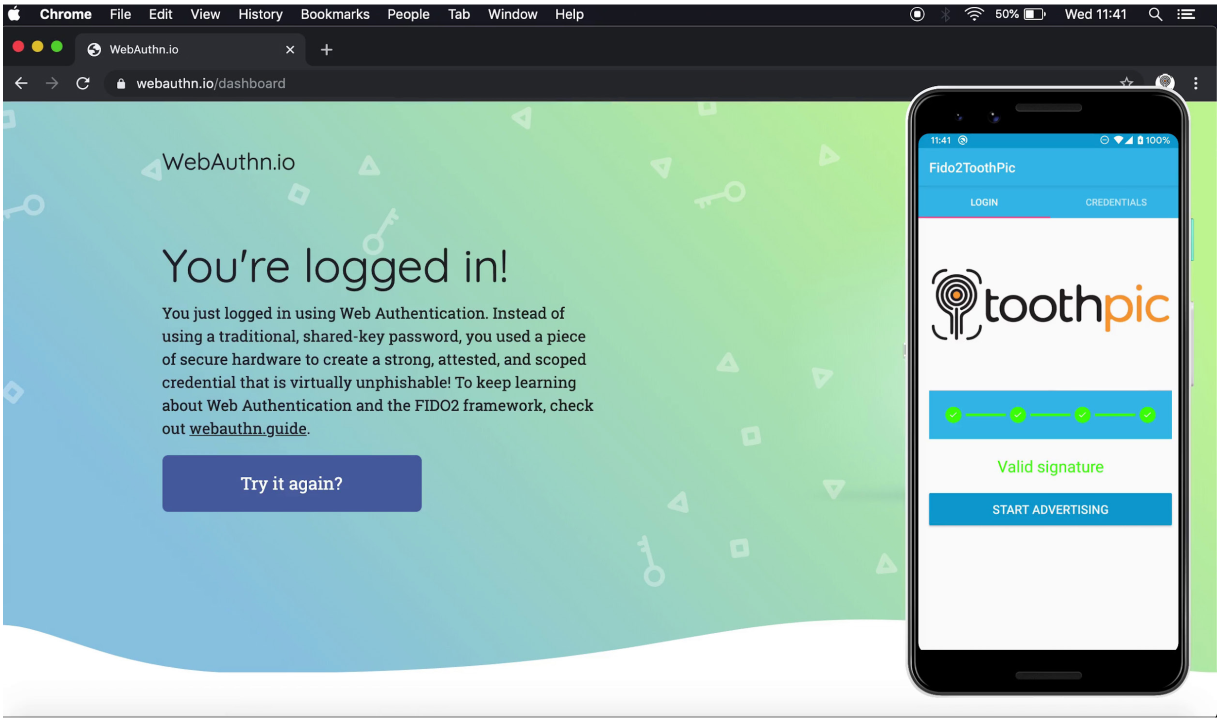
- Processing, storage, and de-obfuscation of secret credentials can be implemented relying on secure areas and secure computation technologies already available on modern smartphones, like a Trusted Execution Environment (TEE). For those devices where a TEE is not available, de-obfuscation of the secret key can be implemented using whitebox cryptography. Moreover, even if the secure area of the device is compromised, this would not compromise the secure credential, since this is obfuscated using ToothPic technology and can only be recovered using the fingerprint of the camera sensor;
- The user does not see the complexity of the technology. The complete authentication process can be started with a simple click and lasts only a few seconds, without requiring any user interaction.



[10] https://fidoalliance.org/

TECHNOLOGY **COMPARISON**

Current vendors of authentication systems propose similar portfolios of MFA technologies, that can be broadly classified into solutions requiring a dedicated hardware (like smartcards, USB tokens or OTP tokens), or relying on smartphones (OTP via SMS, OTP via authenticator apps or asymmetric cryptography-based/FIDO solutions). With respect to existing solutions, ToothPic provides several advantages in terms of security, usability and costs.



WebAuthn.io

You're logged in!

You just logged in using Web Authentication. Instead of using a traditional, shared-key password, you used a piece of secure hardware to create a strong, attested, and scoped credential that is virtually unphishable! To keep learning about Web Authentication and the FIDO2 framework, check out webauthn.guide.

Valid signature

Dedicated hardware

Many services like user authentication or digital signature rely on specific authentication hardware that users should carry with them at all times, for example a token to securely access a bank account or a smart card to sign a document. Such hardware usually is only able to perform specific operations using pre-installed keys. Moreover, some dedicated hardware may have interface problems, for example standard USB tokens cannot be connected to smartphones. ToothPic offers the ability to securely store on an existing personal device the keys required by the above applications, avoiding to purchase and maintain specific hardware. Moreover, due to the flexibility of the key obfuscation technology, even existing keys could be enrolled on the user's device. It is worth noting that in specific economic sectors, like the banking industry, hardware tokens are increasingly replaced by smartphone-based systems.

Smartphone-based systems

Temporary codes sent via SMS/voice call

Despite being available to a very large class of devices, this technology is currently considered obsolete and vulnerable to security threats, since SMS and voice calls can be intercepted by malware. Moreover, the use of the mobile network incurs in additional costs that cannot be easily foreseen by service providers. Even if still widely used, this system has been deprecated and will be superseded soon.

Temporary codes generated by smartphone apps (e.g. Google Authenticator)

These systems have multiple drawbacks. From a security point of view, being based on a shared secret saved on both the device and the authentication server, they present a single point of failure and are vulnerable to server side attacks. Concerning the usability, the user is often forced to cut and paste or memorize the temporary code to complete an authentication form, switching back and forth between different apps, with a quite frustrating experience. ToothPic immediately eliminates any cost related to the management of secret credentials on a centralized server, since users' private keys are only stored on their own devices.

Systems based on asymmetric cryptography

These systems rely on a private key saved on the user's device. When the key is saved unencrypted on the general purpose storage these systems offer very little security, since any user with access to the device can recover the key. Saving the key in encrypted form increases the security, however the key is still vulnerable to online attacks. Moreover, a powerful adversary could try to launch an offline attack and decrypt the key. The usual solution is to save and use the key within a Trusted Execution Environment (TEE). A TEE is a virtualized area of the device, in which the CPU and RAM are only accessible to trusted applications running within the TEE. Executing code within the TEE is safer than in the conventional environment managed by the operating system. However, this is less flexible, since third party applications usually do not have access to TEE. Moreover, being a virtual area, the TEE is vulnerable to software attacks exploiting bugs in the trusted applications. The security can be raised by resorting to a Secure Element, which is a dedicated cryptographic chip. However, this solution has the same problems of increased cost and reduced flexibility encountered with external dedicated hardware. Currently, smartphones embed SEs dedicated to secure payments. Those devices, however, are only able to implement specific cryptographic protocols and usually cannot be updated. ToothPic solves the security problems of the above solutions, since the key is never stored on the device but tied to the sensor hardware. ToothPic can also implement key de-obfuscation within the TEE, offering an additional security layer. Moreover, being based on camera sensors that are ubiquitously present on modern smartphones, ToothPic does not require additional SEs.

MFA Technology		**SMS OTP**	**OTP via Authenticator App**	**Dedicated Hardware Token**	**Smart Card**	**FIDO Phone as a Token**	
Usability		🙁	😐	🙁	🙁	🙂	🙂
Security Index		🙁	😐	🙂	🙂	😐	🙂
Security Threat	*Duplication*	🙁	😐	😐	🙂	🙂	🙂
	Eavesdropping	🙁	🙁	🙁	😐	😐	🙂
	Offline Cracking	😐	😐	😐	🙂	🙂	🙂
	Side Channel Attacks	🙁	😐	😐	😐	🙂	🙂
	Phising/Social Engineering	🙁	😐	🙁	🙂	🙂	🙂
	Endpoint Compromise	🙁	🙁	🙁	🙂	😐	🙂
	Theft	🙁	🙁	🙁	🙁	😐	😐

As shown in the above table, the existing technologies still don’t satisfy the security and usability needs required by a modern authentication platform. The most secure solutions still lack usability, whereas the most versatile ones have significant security flaws. Even the currently available most secure and user-friendly solutions, based on asymmetric cryptography on smartphones, when implemented without ToothPic key obfuscation technology are exposed to smartphone vulnerabilities.

ToothPic solution provides the same security level of dedicated hardware with lower cost, as it can be implemented on a wide range of available commercial devices meeting a minimal set of requirements. ToothPic customers don’t need a huge investment for ad-hoc hardware prone to high obsolescence risk, but they can deploy an authentication solution relying on smartphones that are easily available on the market, or even already owned by their customers or employees.

toothpic

c/o I3P - C.so Castelfidardo, 30/a,
10129, Torino (Italy)

☎ +39 340 290 50 60

✉ info@toothpic.eu

www.toothpic.eu