SIKUR ID

WHITE PAPER

Version: February 2020

find out more at **sikur.com**

1 - About Sikur

The Company

Sikur is defining the future of secure communication, operating globally, through its offices and Distributors in Brazil, the United States, Europe, the Middle East, and Japan. Sikur works alongside governments and corporations that believe security is fundamental to the integrity of their work. We believe that security is not only about platforms and digital systems but is a mindset that surrounds every aspect of a business.

According to Gartner (Market Guide for Secure Instant Communications Report), Sikur is a vendor that has relevant solutions to this technological realm.

The Products

Sikur is the result of a fusion between the most advanced types of technology currently available on the information security market. We are bringing the most innovative form of online technology and privacy while ensuring the messages, calls, chats, and documents exchange in an extremely secure way.

Not just with an encrypted military-grade App, but going one step further, integrating the concept of private cloud and security all the way down to the endpoint. This is guaranteed by the exclusive model for App authentication, its operating system, and software suite with specific guidelines to provide security and privacy at the App and hardware level.

As mobility grows and Digital Transformation takes place, a set of new technologies also appears, and one of them is the IoT (Internet of Things). Sikur has a deep experience in cybersecurity, where IoT is currently struggling to take off once and for all. These same problems that Sikur is solving for companies and governments, through Sikur Messenger, will now be addressed by our new research and development cell in Sophia Antipolis, France, with a focus on IoT.

Sikur Lab (https://sikur.com/labs/)

To keep our most significant asset (the technology), Sikur has established a new R&D center at Sophia Antipolis´s Science Park, a notable and global technology and innovation center near Nice, France. In this same region, Sikur has become member of the SCS Cluster, which is one of the most prestigious cybersecurity centers in Europe, with a focus on secure communication, where we are working inside an environment full of specialized and global companies, accessing high-quality human resources, participating in strategic projects and leveraging our products and technology to a higher level.

Innovation and Future

Our thoughts are not only on Secure Communication solutions but also in a foundation that makes possible shielding communication in different situations. We did invest a lot of time developing a scalable technology, able to solve other problems that could not even be imagined, but which we know that time would bring them to us, like the IoT market and its branches in smart meters, autonomous cars, healthcare, smart cities, and many other industries . By our innovative methodology, we found that there is no challenge to port Sikur technologies to this new market. There must be some customizations, based on our strong foundation, and figured that we would be ready to deliver the best protection for this industry.

We are the foundation. We are the New Secure Communication Mindset.

2 - Abstract

This paper discusses the main aspects of data safety, attack types that affect authentication products, and the protection for them.

It also introduces Sikur ID and its modules (Smart MFA Sikur Data Key and Sikur Chain), explaining their characteristics, strengths, and how each solves a set of problems faced by several industries. It also shows Sikur ID and modules differentials and features, explaining why the solution is safe as well.

3 – Introduction

Reliable authentication systems are the foundation of any modern organization. It is the castle front door, where bad guys usually try to break first. Weak identification systems, easy to crack, and with no side protection is the primary target for various attacks methods. Authentication systems must be robust enough to not touch users' productivity, but also easy to integrate and manage, from the IT viewpoint.

Traditionally, we are all used to access systems by using the username and password pair. Although there are lots of systems still using this method, it can't be trusted anymore. The use of Two or Multi Factor Authentication (2FA or MFA) is a security mechanism widely adopted to make systems safer and sturdier for hackers to break into them. It requires users to verify their identity in two (or more) unique ways before getting access to a system or App. It may need a dynamically generated code, delivered to the user in a uniquely accessible channel; biometric information is also a good option as an authentication factor.

For a long time, companies have tried to strengthen authentication by implementing requirements that make it harder to guess and break, like the password length and the use of special characters. Pushing users to change passwords frequently is also a known technique. A system that deploys only username and password as its authentication method is still vulnerable., that is because users tend to use the same password across multiple systems. Phishing and social engineering techniques have an astonishing success rate, letting users reveal their password, leading to systems compromise.

Two Factor Authentication delivers reasonable protection to user accounts. It ensures that even if a password is compromised, the account cannot be accessed. The attacker must know the second-factor method and must have access to it, such as a dynamically generated one-time password (OTP) or biological token.

MFA requires the user providing two of the following data:

- Something you **know** – the password or pin for an account
- Something you **have** – a physical device such as a mobile phone or a software application that can generate OTP codes
- Something you **are** – a biologically unique feature to you such as your fingerprints, voice or retinas

Cracking the password or pin is what most hackers go after by using tools that automate this task. Accessing a physical token generator or getting biological features is harder and the reason why 2FA is useful in providing greater security for user accounts.

4 – Authentication Vulnerabilities

As the technology evolves, it deprecates what was widely useful a couple of years ago, demanding replacement or improvement. Authentication methods are moving from username and password to multi-factor and password-less mechanisms.

Implementing 2FA increases the difficulty level for hackers trying to get access to user authentication data. It is vital to notice that some methods, as widely proved, by demonstration, are not safe, like SMS codes. Some others, like e-mail sent codes, can also be compromised by a side attack. Even though not recommended, they still have merits for raising the bar a bit and blocking lazy hackers.

There are numerous MFA solutions available, low cost, or even free. It is essential to be aware of the effectiveness of those. We all want to improve security but introducing a weak solution could turn into a breach, opening doors to attacks. The methods below show that, once the user has verified username and password, they are required to enter a second password, system generated, and continuously changing before accessing systems. For a clear understanding, this paper describes below the 2FA methods available and how each works, briefly.

SMS Token: Probably the most common method of implementing 2FA. It sends a unique token via SMS text message, usually a 5-10-digit code after a successful username and password input.

- **Secure Vulnerabilities:**
    - Security – 3rd parties can intercept SMS messages
    - Hardware – physical device required, so if a phone is lost or stolen, the user cannot authenticate, as it is GSM number-based.

E-mail Token: Also, another standard method of two-factor authentication. It is very similar to the SMS method, but typical implementations include having the user enter a 5-10 alpha-numeric token or clicking a link provided in the e-mail.

- **Secure Vulnerabilities:**
    - 3rd parties can intercept security – e-mails and tokens compromised.
    - Redundancy – if the attackers gain access to the user's credentials, possibly they could access email as well and thus get the token.

Hardware Token: Mostly used in enterprise environments but can be used in any system. In this method, the user holds a physical device such as a key fob*, USB dongle*, or other devices that dynamically generates a token for the user. These tokens are generally valid for only short periods, some as low as 30 seconds, and continuously change.
*A small electronic security device with built-in authentication protocols

- **Secure Vulnerabilities**:
    - Hardware – devices can be easily misplaced, forgotten, and lost.

Software Token: Software tokens require the user to download and install an application that runs on their computer or mobile device that dynamically generates tokens or authorize access by a single confirmation. With the rise of smartphones, this method is gaining popularity. Software tokens work similarly to hardware tokens in that they are randomly generated and last a brief period before changing. Developers can choose several different implementations to meet business needs.

- **Secure Vulnerabilities**:
    - Security – when poorly implemented, it is possible to compromise the application used to generate token, without user knowledge.

Phone call: This method of 2FA calls the user once they have authenticated their username and password and provides them with the token. Phone calls are an inconvenient method for the end-user but still viable in some scenarios.

- **Secure Vulnerabilities:**
    - Security – calls can be intercepted, forwarded, or voicemails hacked.

Biometric verification: This method of 2FA is one of the most effective so far; that is because biometric verification relies on something that user is. A unique feature such as the user's fingerprints, face, or retina, verifies that the user is who they say they are.

- **Secure Vulnerabilities:**
    - Privacy – storage of biometric data raises privacy concerns.
    - Security – fingerprints and other biometric data can be compromised and cannot be changed.

The Main Attacks We Protect

- **Brute force:** A brute force attack is an equivalent of trying every key on your key ring, and eventually finding the right one. It is guesswork. Brute force attacks are reliable and straightforward. Attackers put a computer to work, trying different combinations of usernames and passwords until finding one that matches.

  A brute force attack attempts guessing passwords at the attacker's home base, considering that the attacker has encrypted passwords information. Once possessing the data, the attacker can use powerful computers to test a large number of passwords without being noticed, as it is offline.

  Going online, a variant of brute force tries to beat a login function of a system or an application to guess credentials. Since it avoids the need to get encrypted passwords in the first place, attackers can use this technique when attempting to penetrate a system on which they have no prior foothold. As the number of online services grows, data leakage goes in the same direction. So, credential recycling (generally speaking, users tend to use a unique password for many online services) turns out to be a piece of valuable information for brute force attacks, as it reuses usernames and passwords from past data breaches to try breaking into systems.

  Detecting and neutralizing a brute force attack in progress is the best bet. Once attackers have access to the network, they’re much harder to catch and eliminate.

- **Token/Private Key theft**: Access tokens (also known as “session tokens”) refer to a piece of data saved on your computer to let an application understand who you are, meaning that you are logged in. Presumably, once authenticated, it’s what enables the user to stay logged in without having to enter the password every time. Most commonly, these are like “cookies,” but there are many types of access tokens.

  If an attacker can take the access-token and add it to their browser (thinking about a web-based system), the application will remember the browser as logged in. It recently happened on Facebook, where the attacker had the user token, getting the "view as" permission to see their timeline information.

  However, there are a few best practices to be aware of that will help. Implementing multiple security levels is an excellent approach, if at some point, some protection breaks, there will be others to support the system and hold the attackers.

  Performing a new authentication when sending restricted data is a good practice. Banks and E-commerce websites use this technique when asking for payment or transferring values. All session tokens (should) come with an expiration date, and after that the server will no longer accept them. A good practice is setting an expiration of 24 hours or less. If your organization happens to get breached in a method similar to Facebook, the damage would be limited only to users who logged in within the last 24 hours (or whatever you set your expiration to).

  Many websites give a choice between third-party authentication and creating a new account, making things easier for the user. For critical data, such as finance or purchasing, it is best having Sikur ID as the Identity Provider specialized in providing such a service.

- **Man-in-the-middle attack**: A man-in-the-middle (MitM) attack is when an attacker intercepts communication between two parties to eavesdrop or modify traffic traveling between the two secretly. Attackers might use MitM attacks to steal login credentials or personal information, spy on the victim, or sabotage communications, corrupting data. MitM attacks are one of the oldest cyber-attacks. Computer scientists have been looking at ways to prevent tampering or eavesdropping on connections since the early 1980s.

  An attacker uses the MiTM technique to a specific purpose, as a side attack. The goal could be spying on individuals or groups to redirecting efforts, funds, resources, or attention. MitM attacks consist of sitting between the connection of two parties and either observing, capturing, or manipulating data traffic. The attack could be through interfering in legitimate networks or creating artificial networks that the attacker controls. Then, compromised transport gets stripped of any encryption to steal, change or reroute that information to the attacker's destination of choice (such as a phishing log-in site). Because attackers may be silently observing or re-encrypting intercepted traffic to its intended source once recorded or edited, it can be tough to spot.

  Though flaws are sometimes discovered, encryption protocols such as TLS are the best way to help protect against MitM attacks. The latest version of TLS became the official standard in August 2018. There are also others such as SSH. The best methods include multi-factor authentication, as provided by Sikur Smart MFA, as part of Sikur ID, maximizing control and protection over existing authentication schemes.

- **Authentication Replay**: is a technique where an attacker repeats or delays a legitim authentication data transmission and fraudulently reuses it. By using this method, the attacker authenticates himself in a system typically not authorized to do so. It can be part of a masquerade attack by IP packet substitution and considered as a variation of a man-in-the-middle attack.

  The way to prevent it is by tagging each encrypted component with a session ID and a number. Using this combination of solutions does not use anything that is interdependent on one another. Because there is no interdependency, it reduces vulnerabilities. This method works due to a unique, random session-id created for each auth execution; thus, a previous run becomes more difficult to replicate. In this situation, an attacker would be unable to perform the replay because the session ID would have changed.

- **Auth spoofing**: is a variation of the packet injection attack when a malicious party impersonates another device or user on a network to launch attacks against network hosts, steal data, or bypass access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, ARP (Address Resolution Protocol) attacks, and DNS (Domain Name System) server spoofing attacks.

  In an authentication scenario, the problem is that if an attacker can observe the negotiation process, he will know the plain text (challenge text) and its associated ciphertext (challenge-response). Using the message injection attack methodology, the attacker could then derive the keystream, request authentication, and use the same keystream on the challenge text to create a valid challenge-response.

- **Phishing**: it is a cybercrime that targets victims contacting them by email, telephone, or text message by someone posing as a legitimate institution. It tempts individuals to provide sensitive data such as personally identifiable information (PII), banking and credit card details, and passwords. Phishing is an example of a social engineering technique to deceive users. It often lures people by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors, or even faking your company.

  There are several techniques and phishing types, like:

  - Spear phishing: attempts directed at specific individuals or companies. In contrast to massive phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success.

- Whaling: it targets senior executives and other high-profile roles. In these cases, the attacker crafts the content to reach an upper manager and the person's position in the company. The content of a whaling attack e-mail may be an executive issue, such as a subpoena or customer complaint.

- Clone phishing: it is a type of phishing attack whereby a legitimate, and previously delivered e-mail containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attacker replaces an attachment or link within the e-mail with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original. Typically, this requires either the sender or recipient to have been previously hacked for the malicious third party to obtain the legitimate email.

- Link manipulation: is one of the most common techniques, as it misspells or fakes the legitimate web address. When pointing the mouse in the web link, the user can check if it is valid, but when using a mobile device, it won't work, as it does not have this preview feature.

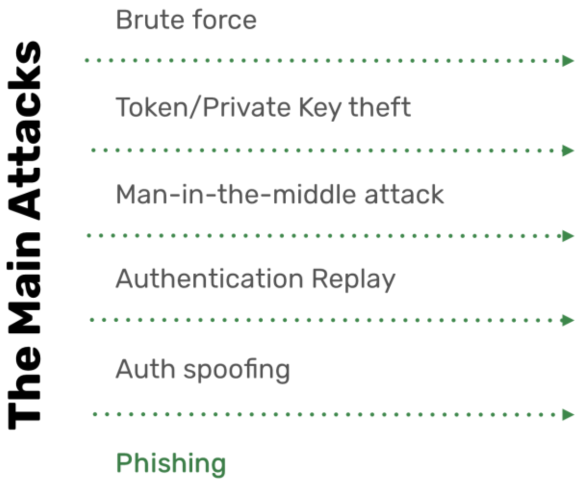


Figure 1: Main types of attacks

5 – The Solution

A persistent problem in technology is related to authentication security. Login with username and password is not enough anymore, and the market demands secure and effective alternatives. Given this widely deployed vulnerable authentication scenario, Sikur ID proposes not only a robust and strong authentication mechanism but also extra modules to increase security, mitigating a set of risks.

The Sikur ID solution relies in a long-term authentication facility, already in use for years on Sikur Messenger and Sikur Phone. It also has been tested over the years by ethical hacking companies, like the world leader HackerOne. So, there is no doubt that it works appropriately, delivering an advanced and safe authentication process. Add to it the Smart MFA, an App by Sikur that plays the 2FA role, which surpasses the existing - and usually hackable - authentication factors like SMS, E-mail, Hardware tokens when it comes do security and convenience.

Sikur ID authentication solution aims to protect the user's private key, which is the most sensitive data when it comes to authentication. Many systems do not handle this piece of information, poorly safeguarding it (sometimes, there is a purpose on it), making hacker's life easier. The private key –

which can eventually be known as system token – does not only identifies the user, but it also defines guidance to systems on which information or parts of the system the user has access. One of the core goals of Sikur ID is keeping it safe with providing several security layers added to the user's strong password and biometric data; by this, the private key is not accessible by third parties.

The Smart MFA also plays an essential role, adding an extra - and necessary – protection to the identification system as a whole. It is flexible, an App that works for the Android and iOS platforms, with secure biometric authentication. Easily replaceable, losing the device will not stop the user from authenticating, just load it in another device, register to match the existing authentication data, and move forward. It is perfect for scenarios where the identity provider is a third-party player. User credentials have a high leak risk (especially for third-party identity providers). When Sikur Smart MFA is in place, the malicious party can't use the auth data to enter the system or App; it will require the second step authentication.

Sikur ID solution is so flexible that it is possible to deploy it in a variety of scenarios, from Client/Server applications, mobile devices, IoT devices, and blockchain. It solves several existing security issues for the IoT market, as default and insecure passwords definition, lack of appropriate management, and data protection with encryption. It also adds value integrating with blockchain applications, delivering compliance by registering and recording all transactions. Figure 2 shows how Sikur ID works.

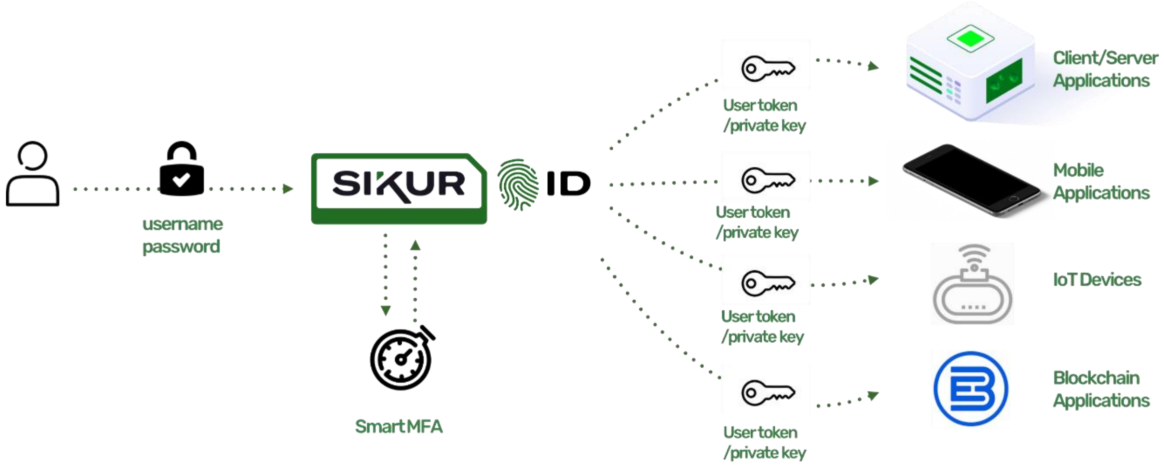


Figure 2: Sikur ID general view

The Product – Modules

- **The Identity Provider:** It is the solution part that holds credentials and performs the authentication process. Many systems do it similarly, but Sikur ID has the expertise on deploying it for a long time, with Sikur Messenger and Sikur Phone. The authentication did pass on several ethical hacking testing, but this is a never-ending process, as it needs constant proving in the App and backend systems as well. While it processes auth information, the private key resides in a cloud-based hardware module, protected with user biometric information so that Sikur or who holds the infrastructure can't open the token and use it to open any sensitive information.

    - A secure user directory for the Organization, safer than username and password
    - It uses a unique authentication process, making use of client's private keys
    - Something unique and that can't be transferred, like biometrics
    - Make use of standard industry protocols
    - Connect the digital identity to the real person by using biometrics, which is something unique

- **Smart MFA:** multiple authentication factors improve security, but even when deploying, it is essential to notice that not all methods are effective, some may also add vulnerabilities, weakening existing systems and Apps. Sikur Smart MFA adds value to existing authentication frameworks and identity providers, like Facebook and Gmail (just to name a few). Smart MFA is an App, signed by Sikur that uses the very same safety layers, like the strong authentication with biometrics and private key protection, making it an excellent choice for those in need to safeguard their user base while increasing security. As it uses standard protocols, like OAuth2, it can easily integrate with existing systems.

  - Improve existing authentication processes
  - Pluggable, easy to connect with your existing system and easy to upgrade
  - Offline: it generates auth codes without Internet connection
  - Take it with you and easily replace it, when needed
  - Make use of standard industry protocols
  - Connect the digital identity to the real person by using biometrics, which is something unique

- **Data Key***: securing the authentication process is the beginning of making everything safe, and the next step is to make sure that confidentiality is in place. The natural path is applying encryption on sensitive data, but it takes more than implementing SSL on top of data traffic to have it encrypted. End-to-end encryption demands proper implementation on several levels, making sure that not only sensitive data is encrypted on transit and at rest, but also ensuring that only the owner has access to it. Sikur Data Key uses the client's private key to encrypt data, making it safer and impossible for any third-party opening private information. Another essential feature is the non-repudiation for information, identifying that data sent and received has source and destination, which can’t be changed.
  - End-to-end encryption using private keys
  - More security: add an extra security layer with encryption
  - Select and encrypt portions of data using our API and your private key
  - Non-repudiation on user data level

- **Chain***: usually a demand from compliance and regulation, the Sikur Chain module delivers non-repudiation at the transaction level, using Blockchain concepts. It uses Sikur ID or Smart MFA keys, ensuring non-repudiation for each transaction. It is possible to grow with Sikur Chain network, adding extra nodes, or building a Sikur Chain private network, with as many nodes as customer needs.

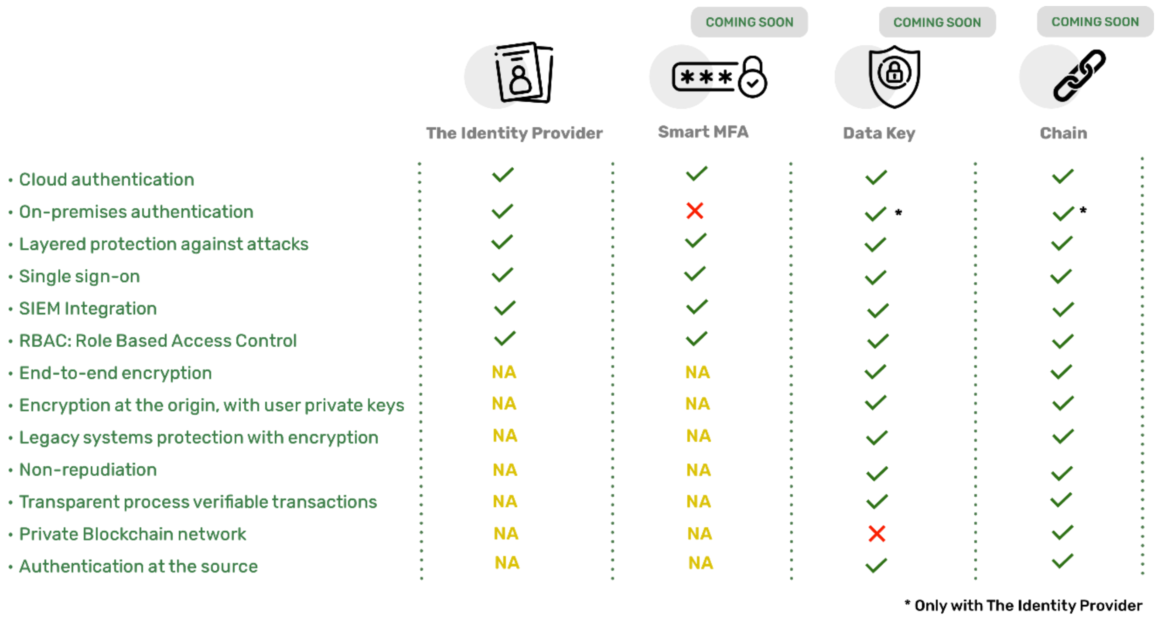
  - Non-repudiation on the transaction level
  - Protect data by registering each transaction, in a transparent and verifiable process
  - Grow safe with Sikur Blockchain network

The Modules – Features

Features make the product appealing, and for Sikur Products, it aims beyond, shielding information with excellent user experience. From Sikur ID to Sikur Chain, all the product's commitment is about fulfilling user needs for safety and compliance. It is what matters the most, running a business that can’t afford data breaches or outages due to security issues.

The feature set in Figure 3 says a lot about the product, how it is structured, and what it paves for future versions. As an Identity Provider, it is ready to deliver the most market needs from authentication with secure 2FA to encryption and blockchain technology, offering main security pillars: authenticity, confidentiality, non-repudiation, and integrity.

Some features are very industry-specific, like SIEM (Security Information and Event Management), which provides logging information to external systems, so that it can provide valuable data to Systems Administrators, subsidizing them for better decision making, like performance monitoring. Single Sign-on is also a desired feature for organizations that want to centralize and ease credential management in an only place. Sikur ID makes it possible. Another unique feature is encryption at the source, which means data protection before leaving the device and by no chance readable by third parties.



	The Identity Provider	COMING SOON Smart MFA	COMING SOON Data Key	COMING SOON Chain
• Cloud authentication	✓	✓	✓	✓
• On-premises authentication	✓	✗	✓ *	✓ *
• Layered protection against attacks	✓	✓	✓	✓
• Single sign-on	✓	✓	✓	✓
• SIEM Integration	✓	✓	✓	✓
• RBAC: Role Based Access Control	✓	✓	✓	✓
• End-to-end encryption	NA	NA	✓	✓
• Encryption at the origin, with user private keys	NA	NA	✓	✓
• Legacy systems protection with encryption	NA	NA	✓	✓
• Non-repudiation	NA	NA	✓	✓
• Transparent process verifiable transactions	NA	NA	✓	✓
• Private Blockchain network	NA	NA	✗	✓
• Authentication at the source	NA	NA	✓	✓

* Only with The Identity Provider

Figure 3: Products features

The Product – Differentials

In a very competitive market, it is hard to set a product apart from other vendors, making it almost an obvious choice for clients. Competitors, when not able to create something valuable and new, most of them work to copy competitors implementing it a bit differently. But, for security products, it is hard to reproduce excellence and protection.

Sikur has long-term expertise with safeguarding the user's private key, keeping it away from any prying eyes and accessible only by its owner. By protecting the user's private key, Sikur manages to deploy data encryption using it; and to get this very same key to implementing non-repudiation is a small step ahead. As the authentication with crucial private protection and proper data encryption takes place, it causes a very desirable side effect: regulatory compliance. That is a relevant set of differentials, indeed.

1. **Private Key protection** - only the user has access to it

2. **Non-repudiation** - Blockchain compatible, control and compliance

3. **GDPR Compliant** - data protection with user keys, private

4. **Protected MFA** - strong and flexible

5. **Legacy systems protection and encryption** - with user private keys, supported by MFA

6. **Business Model** - cloud or on-premises and White Label

7. **Smart MFA** - to solve Phishing

    a. Passwords are the security enemy
    b. Everything is suspicious but your Sikur MFA
    c. Hackers will find a way to bypass fancy AI or ML controls

6 – Why is Sikur ID safe?

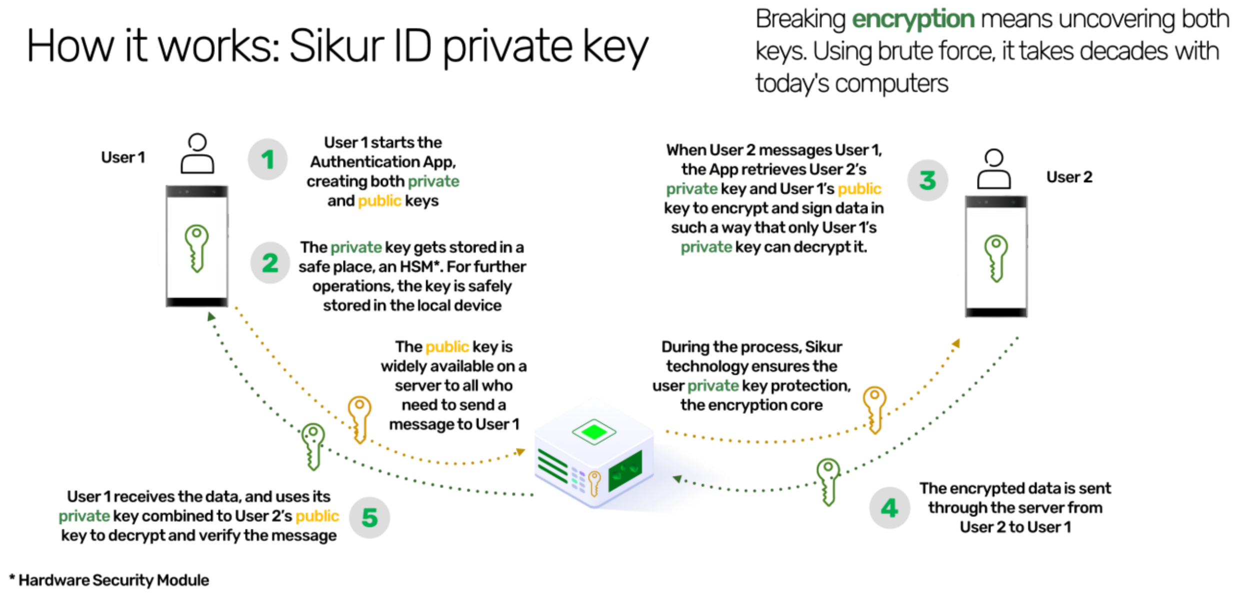
In a short sentence: it is all about keeping the private key safe.

It is not possible to do much when the central piece of information is not decently protected. An authentication system grail is a private key (sometimes called a token) because it opens doors to user information. Sikur ID implements several security layers, as previously mentioned in section 4, making private key protection complete.

A recurrent question is about where and how to store sensitive data, like passwords, secrets, and keys. Sikur products use industry-standard storage equipment for this kind of data, a FIPS-compliant HSM (Hardware Security Module). Building security in a layered approach is also about taking advantage of what is available in terms of cloud infrastructure, like Microsoft Azure capabilities. So, in the cloud level, for public and private clouds projects using Azure, Sikur leverages Microsoft's latest threat management and mitigation protocols, including intrusion detection, distributed denial of service (DDoS) attack prevention, anti-malware, penetration testing, analytics, and machine learning tools to help mitigate threats.

Deploying encryption with the most proven industry algorithms (like RSA and AES) is nothing new, and many vendors do it. Putting its products to the test by ethical hacking companies, periodically, is also good practice; it helps to keep the product up to date and safe from the latest attack trends. Researching and developing new or better ways to safeguard data and mitigating threats as Phishing, like the Sikur Smart MFA, is a task that demands time, effort, and expertise. All of this improves product security, making it safer.

The majority of Identity Providers target user information. So, for them – even claiming privacy and regulatory compliance – accessing personal data (again, claiming anonymity) is part of their businesses. Sikur, as a security provider, has only one goal: keeping user data accessible safe and only available to its owner.



How it works: Sikur ID private key

Breaking **encryption** means uncovering both keys. Using brute force, it takes decades with today's computers

1 User 1 starts the Authentication App, creating both private and public keys

2 The private key gets stored in a safe place, an HSM*. For further operations, the key is safely stored in the local device

The public key is widely available on a server to all who need to send a message to User 1

3 When User 2 messages User 1, the App retrieves User 2's private key and User 1's public key to encrypt and sign data in such a way that only User 1's private key can decrypt it.

During the process, Sikur technology ensures the user private key protection, the encryption core

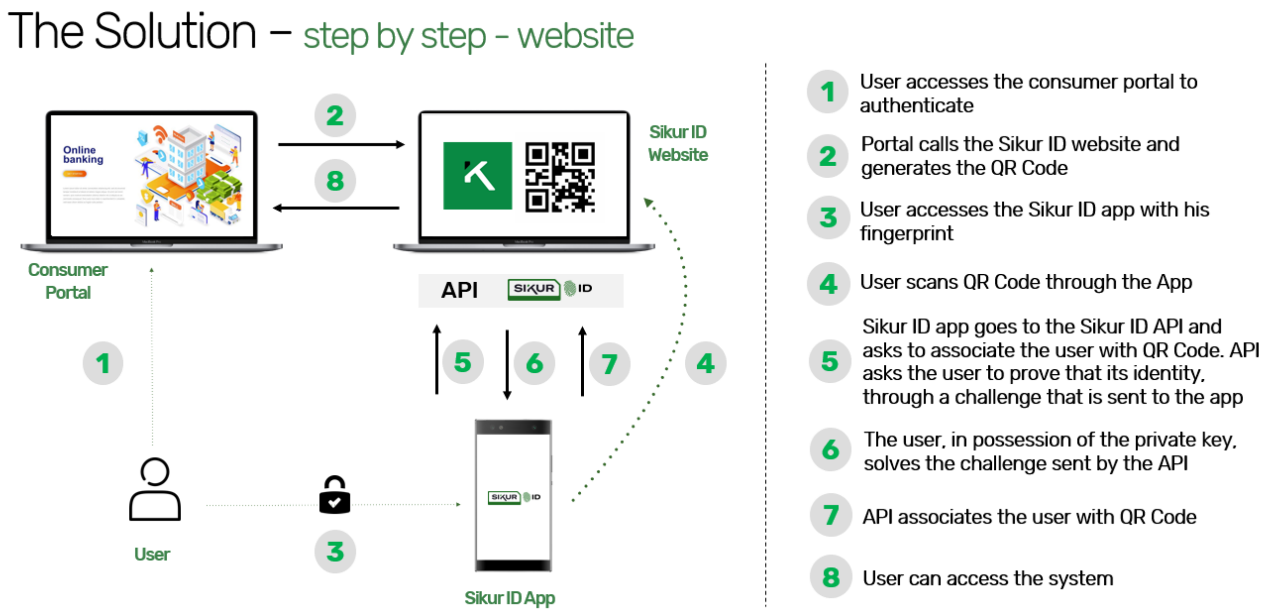
4 The encrypted data is sent through the server from User 2 to User 1

5 User 1 receives the data, and uses its private key combined to User 2's public key to decrypt and verify the message

* Hardware Security Module

Figure 4: User private key protection

An extra example, shown in Figure 5, to consolidate the understanding about how the process works for a web-based authentication, where the authentication App plays a crucial role in the whole process. The scenario is suitable for the Sikur Authentication App or the technology can be embedded on user App by using the Sikur SDK.



The Solution – step by step - website

1. User accesses the consumer portal to authenticate
2. Portal calls the Sikur ID website and generates the QR Code
3. User accesses the Sikur ID app with his fingerprint
4. User scans QR Code through the App
5. Sikur ID app goes to the Sikur ID API and asks to associate the user with QR Code. API asks the user to prove that its identity, through a challenge that is sent to the app
6. The user, in possession of the private key, solves the challenge sent by the API
7. API associates the user with QR Code
8. User can access the system

Figure 5: Web-based authentication process

7 – Results and Conclusion

No doubt, providing secure identity demands not only a set of appealing features, which might be useful and essential to some users but protecting user private keys is crucial. Implementing security layers and, consequently, reducing the attack surface is highly desirable as well.

A product that devotes to exhaust all weakness possibilities, aiming to protect user data like Sikur ID, for sure would be an excellent choice for many types of business verticals. The IoT market demands safety, regulations are coming fast, and the best way to fit and start at the right path is by using a solution like Sikur ID and aggregating value with Smart MFA and its modules.