AUSTRIAN INSTITUTE OF TECHNOLOGY

Digital Identity Management

An AIT White Paper

These days people wish to move both freely and safely; to cross borders swiftly with secure access controls without hindrances; to make transactions payments or access governmental services through quick and convenient proof of identity. We are addressing here the major issues the security discipline and processes.

All the above come with new regulations initiated by the European Commission as the new GDPR (General Data Protection Rules).

Introduction

Identity Management (IDM) is the organisational key process for identifying, authenticating and authorising individuals or groups of people to access applications, systems or networks by associating user's rights and restrictions with established identities. The managed identities can also refer to software processes that need access to organisational systems.

Authentication

It is widely agreed that the first step of action for verifying the identity of a user or process is through the control access and proof of identity (authentication). To establish this process three main categories (factors) are used:

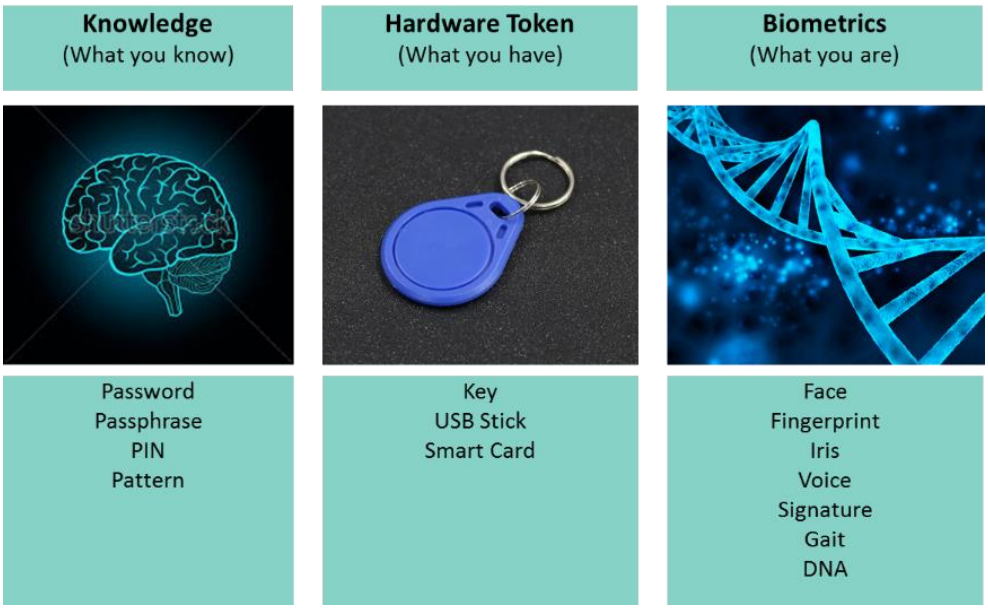


Figure 1. Three different authentication factors, source: AIT

Something you know

Knowledge factors are the most commonly used form of authentication. The user is required to prove knowledge of a secret to authenticate him. A "password" is a secret word or string of characters that is used for user authentication. Variations include both longer ones formed from multiple words (a passphrase) and the shorter, purely numeric, Personal Identification Number (PIN) commonly used for ATM access. Traditionally, passwords/PINs are expected to be memorised.

Something you have

Possession factors ("something only the user has") have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession factor authentication in computer systems. Chip Cards are examples of tokens.

Something you are

Inherence factors are associated with the user, and are usually biometric methods, including fingerprint, facial, iris, and retina or voice recognition.

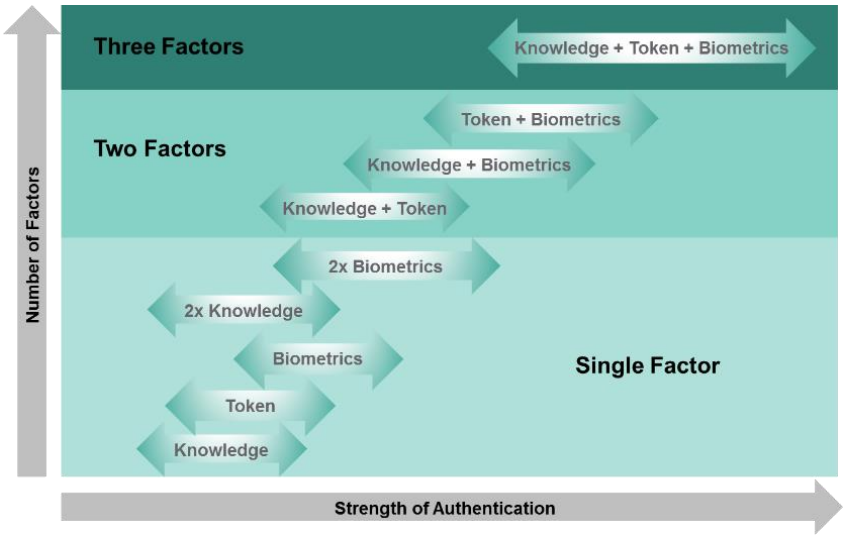


Figure 2. Single, two and three factor authentication strength overviews, source: AIT

Multi-Factor Authentication MFA

Multi-Factor Authentication (MFA) is a method of confirming a user's claimed identity for which a user is granted access only after successfully presenting more than one piece of evidence or factors to an authentication mechanism. The higher the number of factors the higher the authentication strength. Two-Factor Authentication, also known as 2FA, is a subset of Multi-Factor Authentication. It is a method of confirming a user's claimed identity by utilising a combination of two different factors. A good example of two-factor authentication is the withdrawing of money from a ATM; only the correct combination of a bank card, something the user possesses, and a Personal Identification Number PIN, something the user knows, allow the transaction to be carried out.

Mobile Phone Two-Step Authentication

Mobile Phone Two-Step Authentication was developed for mobile phones and smartphones to provide an alternative authentication method to avoid memorisation as well as stealing of passwords. In order to authenticate themselves users would use their personal access codes to the device, i.e. something only the individual user knows, plus a one-time-valid dynamic passcode, typically consisting of 4 to 6 digits. The passcode can be sent to the mobile device by SMS, push notification or can be generated by a one-time-passcode-generator (OTP smartphone app). In all three instances, the advantage of using a mobile phone is there is no need for an additional dedicated token since users tend to always carry their mobile devices with them. Many Internet companies like Google, Amazon and AWS use open Time-based One-time Password Algorithm (TOTP) to support two-step authentication.

Biometrics in Smartphones for Device Access

Biometrics in smartphones for device access is increasingly needed, as the omnipresence of smartphones in our daily live is an undeniable fact. It is most important to secure access and data for these technological gadgets. When we enter simple 4 digits pin codes or patterns to unlock sensitive information in our smartphones we do not realise the potential hazard. For companies IT infrastructure operators, protecting smartphones has become an ordeal, resulting in more restrictive policies requiring entering lengthy passwords and closed shop applications leading to a myriad of questions on the smartphone: "do you really want to give access to ….?". The big players have realised the problem and are developing fast and secure device access via biometrics starting with fingerprints, followed by face and now by iris information as a means of authentication on the device itself. Many companies view biometrics as a secure and convenient alternative to complex passwords. Since then there is already on the market a number of smartphones with iris authentication. Once a user registers his iris information, it is stored as an encrypted code. Once a user wants to access

content, such as a protected app, the IR-LED (infrared light emitting diode) and a special iris camera operate together capturing the iris pattern for recognition, extracting and digitising the pattern, and comparing the digitised pattern with the encrypted code in order to verify access. Securing the iris code on smartphones is the task of the manufacturer. The strength of this technology will be to provide new services to companies seeking to manage access to private applications for banking institutions, access control and documents files security via biometrics.

This can either be voice recognition, facial recognition or any other biometric trait captured with special sensors (fingerprints, iris). One example is with the new Samsung Flow application. There is a new possibility to unlock your PC with a fingerprint scanner on your smartphone. In principle, this can be done with any biometric trait. This is only the beginning. As developers start to make use of the device's onboard iris scanner, big players are enabling access to these functionalities allowing verification of transactions and other activities. Technology will expand to various industries like looking into your phone and opening a door. All these solutions will need access to the verification application on the phone and relies completely on the consideration of the manufacturer to free up their identity authentication solution. Some are closed shop for now, only the company can provide the payment app. If you entrust your smartphone, the manufacturer, the Internet provider, the operating system, the apps and the enrolment procedure, everything will be fine.

Biometrics on Special Devices

When linking authentication to biometrics, one possibility is to use special devices. *EMV*, which stands for *Europay*, *MasterCard*, and *Visa*, is a global standard for authenticating credit and debit card transactions that involves chip-compatible cards and point-of-sale (POS) terminals. *EMV* technology has been around for years, and is widely accepted in Europe and around the world. Last year Mastercard announced a smart card which incorporates a fingerprint sensor directly on the card. The clue is that the comparison to the fingerprint of the card holder is compared on the card itself, so no biometric information is leaked outside the card which are typically common criteria certified up to level 6 and more – in fact very secure. The only problem is that biometrics with only one finger have not the best false acceptance rate / false rejection rates (FAR/FRR).

Other examples are access terminals, usually used with a chip card to gain physical access. Recently, more and more combinations with biometrics are entering the market; equipped with fingerprint scanners, facial scanners, palm veins and iris.

Figure 3. Access Terminals:
Fingerprint (Morpho/Idemia), Palm Veins (ZKTeco), Face (Ness Cooperation) and (Iris ID)

Issues and Shortcomings in Today´s Systems

Weak Knowledge Factor (password/PIN) Security

Authentication should be fast and convenient for easy memorisation so users reduce PINs and passwords complexity. Most commonly used passwords are a combination of nicknames and numbers (often dates), researchable words (birthdays, monthly changing numbers enumerated by month, names of friends, pets, etc.) Many secret questions such as "Where were you born?" are examples of knowledge factors weakness because they may be known to a wide group of people, or be able to be researched.

Password or PIN memorisation for elderly people is also a bigger problem. People with the need of memorisation for several passwords in different systems/accounts memorisation are definitely a problem and the tendency has become to write them down. It should also be noted that the enforcement of stronger passwords by policy does not prevent the use of meaningful information in the password nor suppress the reuse of the password over multiple systems.

20 Of The Most Popular Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17. dragon
18. passw0rd
19. master
20. hello

Trust in Biometric Data Storage, Security and Privacy Concerns for Biometric Identity Servers.

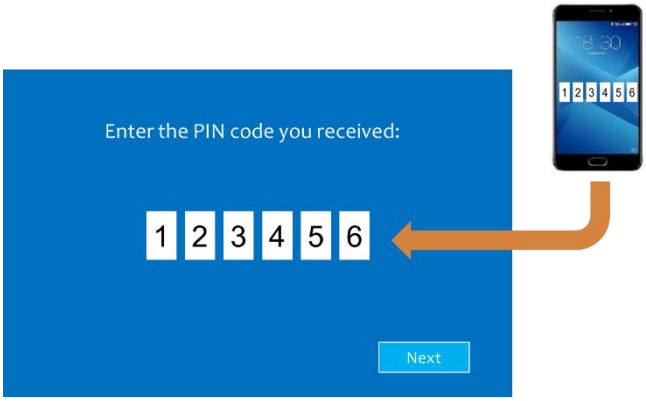
Recent hardware flaws found in mass market CPUs like with “Meltdown, Spectre”, affect directly the chips and let hackers bypass the hardware barrier between applications run by users and the computer’s memory, potentially letting hackers read a computer’s memory and steal passwords. In servers like cloud-based systems, several applications from various users sharing the available computers, can possibly access data from other users. The list of attacks on cloud-based systems with huge amounts of data loss is rather extensive. In 2017 alone incidents happened with multiple companies. Equifax had a breach affecting 143 million US consumers. Deloitte had a breach where “hackers had potential access to usernames, passwords, IP addresses, architectural diagrams for businesses and health information” of 244000 staff. Disqus announced 17.5 million users' email addresses, login names and, for about a third, passwords had been salted and hashed with SHA1 been exposed.

The list of hacks and cracks is also extensive, introducing vulnerabilities and possible future data leaks. Again the list is incomplete and only of recent vulnerabilities: Cloudbleed (2017), Broadcom Wi-Fi (2017), EternalBlue (2017), DoublePulsar (2017), Silent Bob is Silent (2017), KRACK (2017), ROCA vulnerability (2017), BlueBorne (2017), Meltdown (2018), Spectre (2018).

Disadvantages of Mobile Phone Two-Step Authentication

Mobile phone apps, SMS, and direct push notifications, etc., are not considered "something you have" thus are not considered in the multi-factor/two-factor equation. Mobile phone two-step authentication is more secure than single-factor password protection but suffers some security concerns. Mobile phones can be cloned and apps can run on several phones; mobile phone maintenance personnel can read SMS texts. In particular, mobile phones can be compromised in general, since it is no longer guaranteed the mobile phone is something only you own entirely.

The major drawback of authentication is the user must at all time carry with him the physical token such as the USB stick, the bankcard, the key or similar. The loss and theft of such tokens are a risk. Due to malware and data theft-risks as well as equipment not having USB ports, many companies' security policies forbid user to carry an USB and an electronic devices. Physical tokens usually do not scale, typically requiring a new token for each new account and system. Procuring and subsequently replacing tokens incur additional costs. Furthermore, there are inherent conflicts and unavoidable trade-offs between usability and security.



- User must carry a charged mobile phone, kept in range of a cellular network, whenever authentication might be necessary. When the mobile phone is either unable to display messages, damaged or shut down during the update of the phone or due to extreme temperatures (e.g. winter exposure), access will often be impossible without backup plans.
- Use must share their personal mobile number with the provider, reducing personal privacy and potentially allowing spam.
- Mobile carriers may charge the user for messaging fees.
- Text messages to mobile phones using SMS are insecure and can be intercepted. Thus, third parties can steal and use the token.
- Text messages might not be delivered instantly, adding additional delays to the authentication process.
- Account recovery typically bypasses mobile phone two-factor authentication.
- Modern smartphones are used both for browsing emails and receiving SMS while Email account are often always being logged in. The problem resides when the phone can receive the second factor on the logged in email account while the mobile phone is stolen or lost. Smartphones combine the two factors into one factor.
- Mobile phones can be stolen, potentially allowing the thief to gain access into the user's accounts.
- SIM cloning gives hackers access to mobile phone connections. Social-engineering attacks against mobile-operator companies have resulted in the handing over of duplicate SIM cards to criminals.
- Security of mobile-delivered security tokens depends fully on the mobile operator's operational security and can easily be breached by wiretapping or SIM cloning by national security agencies.

User Convenience and the Right “to-be-forgotten”

Finally, authentication systems should provide user with fast, secure as well as convenient access to various (physical) services. Should raise security level for payment transactions with two step/factor, smartphones based systems might be convenient but those systems require additional infrastructures such as providers, fast and steady online capabilities, data protection during transmission, centralised administration and more. Yet the simple PIN problem remains unsolved. According to the new data protection law for Europe (GDPR), the user has the right to store his data, although the implementing of the “right-to-be-forgotten” cannot be achieved easily.

Emerging Technologies

In most cases we are still at the prototyping phase, future-looking forms of biometric identification include software intelligence systems capable of analysing the way a human users move their mouse or the way they behave with their touchscreen or keyboard. The analytics engine behind this intelligence is capable of tracking tiny variations in speed, movement pattern and, in some cases, pressure – all these factors can be combined to create a ‘unique' profile for an individual user.

Other still-nascent biometric identification systems track heart rate through wearable wristbands. Widgets seen for their most part in the movie industry like iris and retina recognitions are now getting great attention. Biometrics-on-the-fly, the latest buzzword, describes technologies where biometric traits are captured while the person is moving (fingerprints, face or iris). Soon, we will be able to add vein-pattern recognition as means of identification and detect structure and arrangement of human veins.

Recently, private industries have identified opportunities to provide authentication services by marketing secure proof of identity. Resulting in outsourcing user’s authentication and necessitating the creation of an identity provider creating, managing and maintaining identity information enabling single-sign-on (SSO), one and the same authentication for several services reducing password cumbersome.

The question is to know how do you trust this identity service provider? What happened when they are hacked? The latest counteractions are using distributed ledgers in combination with block-chain technology (DLT). A distributed ledger is a consensus of replicated, shared, and synchronised digital data geographically spread out across multiple sites, countries or institutions. There are no central administrator or centralised data storage. A typical implementation is the crypto currency Bitcoin.

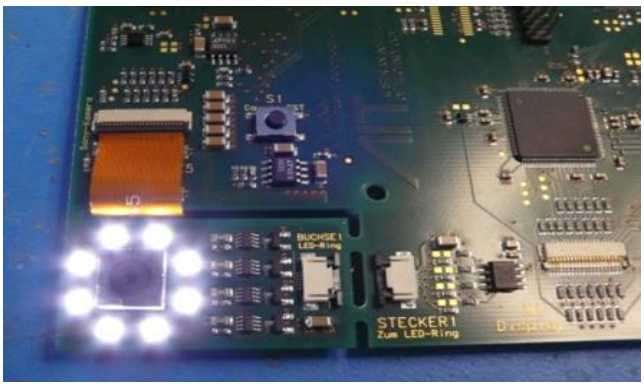
In fact, with blockchains, every public key can now have its own address. This address is called a decentralised identifier. DIDs provide a standard way for individuals and organisations to create permanent, globally unique, cryptographically verifiable identifiers entirely under the identity owner’s control. Unlike a domain name, IP address, or phone number, a DID is not rented from any service provider, and no one can take it away from whomever owns or controls the associated private key. DIDs are the first globally unique verifiable identifiers that require no registration authority. Public blockchains (e.g. Sovrin) can provide decentralised registration and discovery of the public keys needed to verify digital signatures.

AIT Research: Contactless Fingerprint Capturing

Based on our experience in the field of smart border control, and as a coordinator of major EU-funded projects in this context (e.g. FastPass, MobilePass), we develop solutions and prototypes for identifying individuals on the move. We combine ingenious algorithms with 3D stereo data to create access control solutions ranging from low to high security applications. We implement contactless biometric solutions for mobile devices to ease the work of Law Enforcement Agencies and other safeguards. This new approach for the contactless capture of fingerprints using a mobile device enhances security, speeds up the border control process, makes biometric verification less cumbersome to individuals and officials.

Figure 4. Demonstrator of contactless and mobile fingerprint verification, source: AIT – European FP7 project MobilePass, www.MobilePass-project.eu

AIT developed a dedicated, secure and mobile device for Law Enforcement Agencies (LEAs) to use in biometric identification and for inspecting travel documents on the move. A typical application is border control on land borders or trains. The platform combines leading edge technologies, such as contactless fingerprint scanning, facial verification, optical passport scanning and passport chip reading. In contrast to existing mobile solutions, the hardware itself is a trusted platform module with encrypted operating systems and applications. 3G/4G, WiFi and Bluetooth connectivity ensures interoperability with other IT systems. The developed system is based on a Multi-Processor System On Chip (MPSoC) design with enough processing power, paving the way for future apps including iris scanning.



The capturing system for fast fingerprint capturing (4 fingers at once) is patented pending. Similar technology was used to capture 4 fingers with the phone camera of a regular smartphone.

AIT Research: Contactless Veins Capturing

One of the most challenging biometrics to capture is the palm vein pattern or fingers. Palm vein authentication technology utilises images captured by illuminating a palm with the safe near-infrared band light, which passes easily through the body. The haemoglobin in the palm veins absorbs this light, thereby reducing the reflection rate and causing the veins to appear as a black pattern. Accordingly, a palm vein authentication device's optical unit consists of an illumination component and an image capture component. To uniformly illuminate the entire palm, the illumination component, the widest part of the optical unit, is arranged to surround the image capture component. To improve the convenience of the user different methods are in development to capture the distance, the form and orientation of the palm to speed up the capture process while giving maximum freedom for the hand positioning.

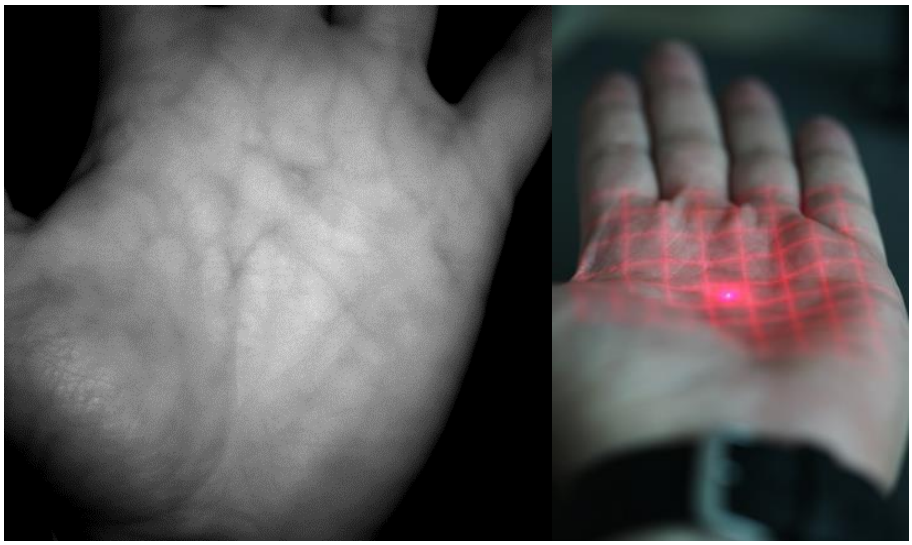


Figure 5. Demonstrator of palm vein capture unit, and test for 3D measurement of palm form characteristics, source: AIT research

AIT does research on the capturing technologies, e.g. the way how the system knows what the best biometric sample to use for verification/identification is. The AIT approach uses a real-time system which permanently tries to capture the biometric trait, investigating in the quality of the captured image and replacing the image if a better one is taken in the next moment (we call it best-shot analysis). In addition, a specialised system, combining an ultra-fast absolute positioning lens with a high-speed camera, ensures that images are sharp. This technology is also used for extremely fast fingerprint capturing on-the-fly where fingers are not in the same distance to the camera – and obviously – would need different focus adjustments.

AIT Research: Iris matcher on card

Biometrics has gained acceptance as a legitimate method for determining an individual's identity, ensuring high security standards and facilitating the process authentication. The one problem remaining unsolved is the biometric template, which needs be stored somewhere to be checked against. Biometric data must be secured at very high level against any misuse leading to identity theft. Storage is typically done in a server, recently provided by newly established identity providers, and sometimes directly on an access control device. All countermeasures, encryption, distributed storage, have a single weakpoint which occurs when the biometric information is revealed. In addition, the devices/servers and their software are been exposed to external threats like rooting or infiltrating (see Meltdown and Spectre hardware breaches).

Today the biggest issue for IT systems is the protection of private data, especially biometric data. The list of recognised security breaches goes on and on. Independent of the method (hacking, phishing, highly complex technical fraud) every breach is a disruption of trust in the technology. For a secure and convenient identification of individuals we propose a very strong 2-factor authentication system, which is a so-called Matcher-on-Card solution for Iris biometric data.

A radical new approach is foreseen where the biometric information never leaves the device (e.g. a token, a keyfob) via a so-called Matcher-on-Card (MoC) solution. During enrolment, the biometric information is transferred onto the chipcard, keying the card to the biometric trait and thus the user. During identity verification, the actual biometric trait is given to the card and a new on-board-matcher (the card itself) decides if the presented biometric information and the biometric trait stored on the card are the same, enabling access or other identity related actions.

Advantages of an Iris Matcher-on-card system:

- very high authentication strength: card as token and iris as biometrics factor
- biometric data never leaves the card, protected by a high-sec chip module (CC6+)
- privacy-by-design: only the user owns his data; "right-to-be-forgotten" is implemented
- anonymisation: white label cards (key fobs) give no traces to the user (no photo/text)
- a stolen card is useless without biometrics, stolen biometrics useless without card
- Additional security layer by sophisticated template protection (e.g. homomorphic enc.)
- no password memorisation needed

GLOSSARY

ATM	Automated Teller Machine
CC	Common Criteria Certification
DLT	Distributed Ledger Technology
DID(s)	Decentralized Identifier(s)
EMV	Europay, MasterCard and Visa
GDPR	European Commission General Data Protection Rules
IR-LED	Infrared LED (Light Emitting Diode)
IdP	Identity provider
Keyfob	Key Chain or similar, equipped with RFID to (e.g.) open a door
MPSoC	Multi Processor System On Chip
POS	Point of Sale
SHA-1	Secure Hash Algorithm 1
SSO	Single Sign On
SIM	Subscriber Identity Module (SIM Card)
TOTP	Time-based One-time Password Algorithm

About AIT

AIT is Austria's largest Research and Technology Organisation (RTO) and belongs to the first league worldwide in many of our areas of research. This makes us a powerful development partner for the industry and one of the top employers in the international scientific scene.

AIT is strategically positioned as a key player in Austrian and European innovation system by performing applied research and enabling the market exploitation of innovative infrastructure related solutions. The functionality of “bridging the gap" between research and technology commercialisation is a key aspect of developing new technologies and enabling an economic boom. Regarding the Austrian innovation landscape, AIT fulfills this role by its new orientation, in providing a research environment to help key industries facing mid-to-long-term challenges. Unlike universities that are focusing on basic research and addressing short-term exploitation, AIT covers the entire spectrum from taking up emerging technologies, first proof of concepts, applied research to transferring these emerging technologies into specific applications up to demonstrators and prototyping.

This allows AIT to connect basic research and the usage of new technologies for the industry and thereby pave the way for commercialisation.

Publication Date: March 2018

Bernhard Strobl
Thematic Coordinator Digital Identity Management
Center for Digital Safety and Security

AIT Austrian Institute of Technology
Center for Digital Safety & Security
Giefinggasse 4, 1210 Vienna
www.ait.ac.at