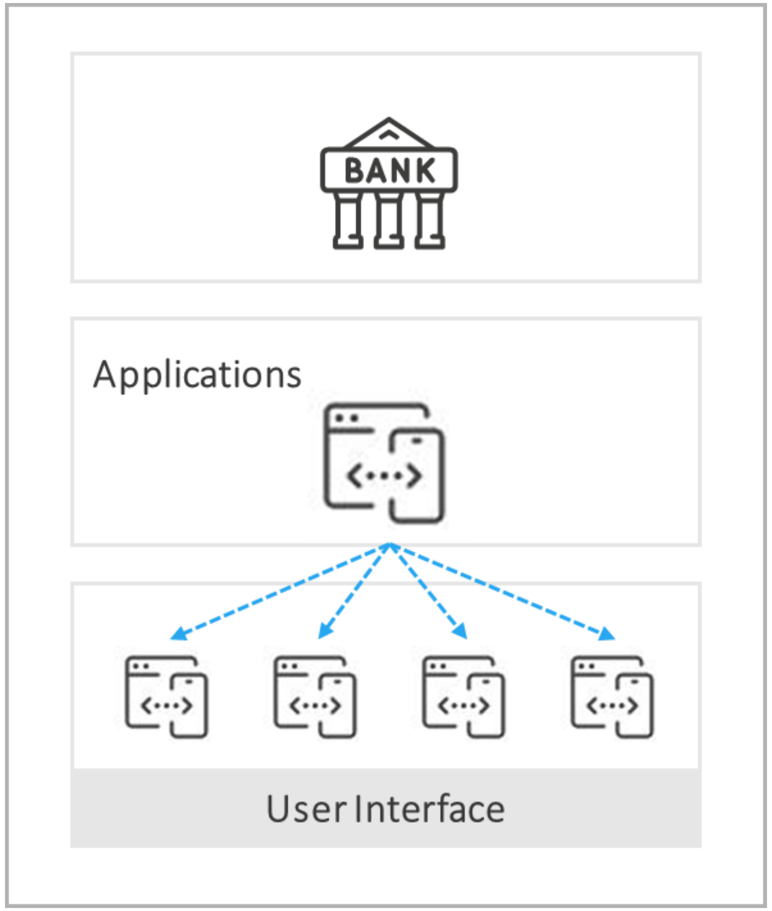
UBISECURE™

The Definite Guide on Authentication for Applications

UBISECURE WHITE PAPER



Online services, applications, need to authenticate their users properly. Authentication is a process where the identity of the visitor is established. In an optimal situation this identity will travel with the user both within the application and can be transferred to another application through technology called federation.

> *"An application program (app or application for short) is a computer program designed to perform a group of coordinated functions, tasks, or activities for the benefit of the user."* -
> https://en.wikipedia.org/wiki/Application_software

Within a single server or in an online service that looks unified and consistent to the end user there can be multiple applications. An online bank can present a very harmonious front-end to the customer, but insurance, account operations, loans etc. most probably are different applications. Each of these applications need to know the identity of the customer. An often used term "relying party" or "service provider" describes this front-end experience, or encompasses all the applications the example bank is running, but not the application itself. Another good example is Microsoft Office. People ask "are you using Office?" instead of the application(s) it consists of. Therefore we refer to the application in this paper when we talk about the entity that needs to know the identity of the user.

This is the traditional view. Right now we live in a time when devices are getting smarter and start performing coordinated functions, tasks, or activities for the benefit of the user. This is what we call the Internet of Things. When we examine different authentication methods we'll also consider their suitability to authenticate not only users, but also things. Things are also running an application or applications.

Authentication can be seen as a necessary evil, especially when we talk about stronger authentication than password. The perception is that it is an inconvenience and a cost factor. However, properly deployed authentication for the applications can increase conversion and trust, improve retention, save cost and take the user experience to a new level.

Driving Forces Towards Passwordless Authentication

Everyone agrees that password based authentication is not the best in terms of usability nor security. But password based systems are inexpensive to implement, and you don’t have to train your end users with a new technology or process related to the credentials and their management.

Customer Experience

Digitalization, online services, e-commerce all talk about the customer experience and the customer journey. Personalization is a hot topic. New concepts are created and digital officers and their teams think of new and better ways to improve the customer experience. Quite often the identity of the user, or how it is managed is left out of the picture, designers realizing few months before the launch that they need to somehow capture the identity of the visitor. The result can be a hastily added user database using a complex online registration form and creating yet another password for the user. One of the biggest reason for cart abandonment is the registration process.

Online visitors already have a digital identity, most likely quite few of them. Allowing the visitor to use something that they already have to register can minimize abandonment rates and increase conversion resulting in immediate improvements on the bottom line.

Regulation

Password is not a strong authentication method. Some verticals are facing regulatory pressure to implement strong authentication for their applications. The best example would be the Payment Service Directive 2 (PSD2) within the European Union that clearly states that (under certain conditions) financial transactions must use strong authentication. Industry standards and local legislation such as PCI-DSS 3.2 standard for the payment industry and HIPAA legislation for the US healthcare industry are pushing organisations towards strong authentication. When we discuss about different ways to authenticate a user in this paper we'll try to highlight the suitability of the method category in relation to a regulation or standard.

Breaches

When a secret is stored somewhere outside of the users control, e.g. in a database, it becomes vulnerable to a breach. The past few years have shown us that breaches happen on a daily basis and only the biggest ones break the news barrier. Moving away from an authentication method that requires centralized storage of the secrets is something that online services could benefit from. On the other hand the users, when they create a new account, put a lot of trust in the service provider, but they don't know how their secrets are being handled. The most flagrant mistake a service provider can do is to store the user password (and other identity attributes) in a plain text format and not use server side certificates to protect the communication channel between the user's browser and the online site.

Level of Assurance

The concept of “Level of Assurance” (LOA) is very important when we discuss about authentication methods. NIST (US), the European Union, individual nations and other organisations such as GSMA, have created categories against which an authentication method is evaluated. Higher scores mean more trustworthy digital identities (and authentication). The assurance of an authentication method can be divided into two; Registration process of the identity and the method itself.

When we calculate the overall LOA score, the lower score of registration or method will determine the final LOA for the authentication method and digital identity.

Registration

When we evaluate the assurance level of an authentication method we must first begin by determining how the digital identity was created. Digital identities that are used to authenticate users have different ways how they come to be. Low level of assurance identities do now require any kind of vetting of the true identity of the user. Examples of these kind of identities include social media (Facebook, LinkedIn, Google, Twitter etc.) and the typical registrations to discussion forums, sites, etc. where the user can pretend to be Clark Kent as none of the identity attributes are verified.

On the other end of the scale we have registration processes where users have to visit a branch or government office and show their valid government issued ID in order to get the digital identity issued.

Strength of the Method

The world is full of different technologies on how to authenticate a user. Each authentication method technology will be resistant to discovery, i.e. someone finding out the secret. This resistance can be evaluated and given a score.

Digital identities that rely on the user memory (passwords, secret questions) are at the low end of the scale. When publicly evaluated algorithms such as RSA and ECC for Public Key Infrastructure (PKI) are used the secret can be considered stronger. Then we must also consider the “vehicle” of the identity. Passwords are stored in a database and can be discovered in bulk by breaching the database and e.g. brute forcing the passwords. PKI private keys that are stored in a certified (e.g. EU CWA-standards) environment and using certified software can be considered highly resistant to discovery. A good example is a government issued electronic identity card (smart card).

Phishing is a persistent problem in organisations. Even with constant testing and training of the employees, cleverly crafted phishing mails can be used to discover the secret – if it possible for the user to give out. Authentication methods that do not allow the end user to divulge the secret through a mistake or intentionally are well suited for minimizing risk of phishing attempts, and of course protecting access to confidential information.

Authentication Methods

In this paper we will concentrate on the most common authentication method / digital identity categories. As we go through the categories we will shortly describe the usability of said method to e.g. regulation or Internet of Things usage. At the end of this paper you'll find a table collecting this information in an easy-to-digest format.

In order to keep this paper within reasonable limits in terms of page numbers, we'll have to be fairly brief on each category.

Passwords

As one of the most ancient and widespread methods of verifying user identities, passwords are almost everywhere. The biggest benefit of a password based system is that it is extremely cheap to implement. All that is needed is a simple form where a username and the password is created when registering, database for storing the username and password (in encrypted format, please), and afterwards the login process is simplicity itself. The simple and straightforward implementation of a password based authentication system is its biggest benefit.

Password authentication was invented when you had one or maybe two applications (operating systems) where you needed to restrict access. This method was never intended to be used on the modern Internet where users have accounts in dozens of online services.

After you have implemented a password based system you have several issues to resolve. The first and the most obvious thing is to never store passwords in plain text to your password database. This is still something that some applications do. Fortunately this behaviour is very rare in 2016. The next obvious step is to use HTTPS instead of plain-text HTTP when the user is communicating with the application to encrypt the channel between the e.g. browser and the application. Unfortunately this is something that happens every once in a while .

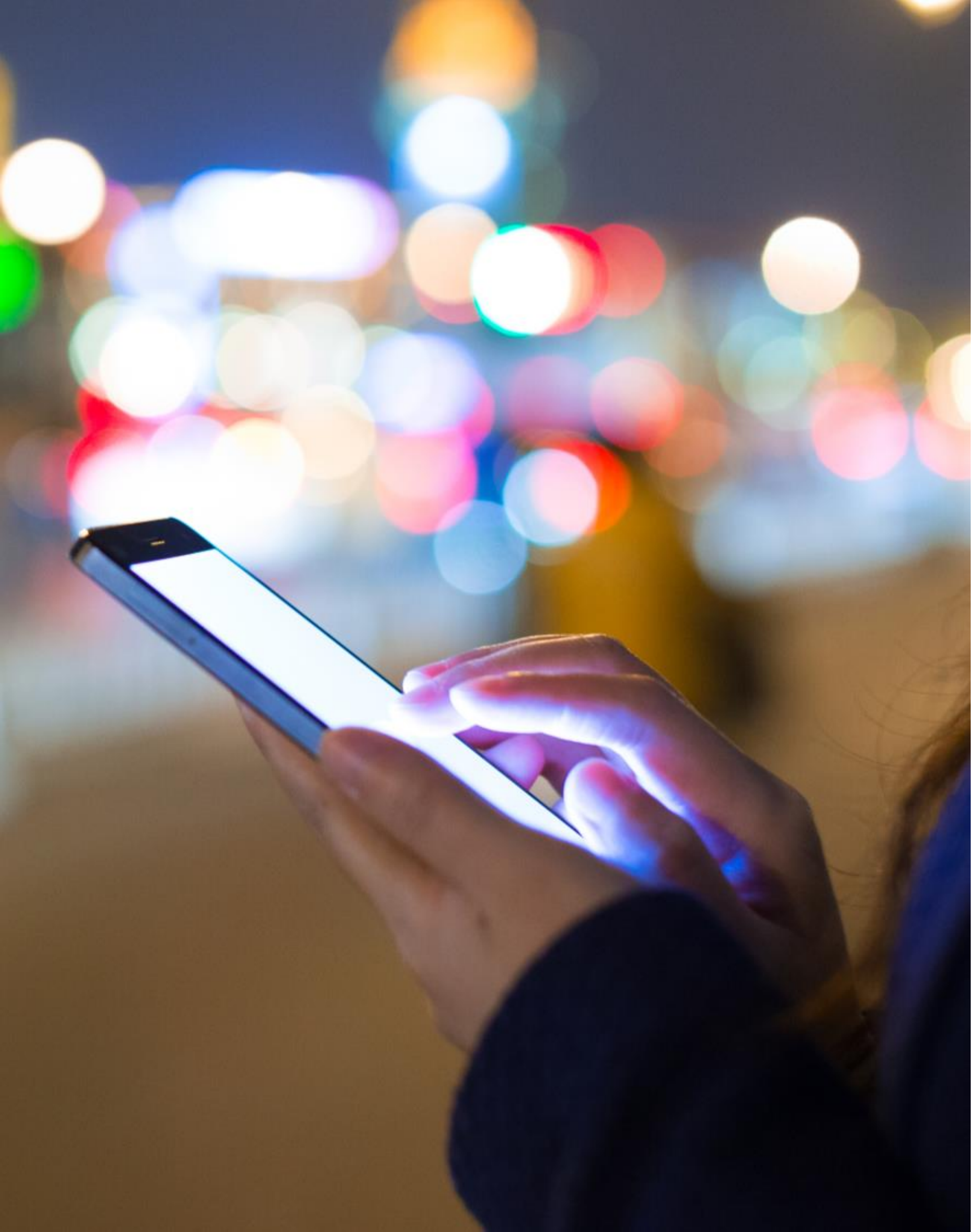
People forget. This maybe the biggest disadvantage a password system has. Trying to keep up with the 65 different passwords you have among different sites, both personal and business, leads to e.g. following user behaviour and diminished security:

- Reuse of passwords across the sites
- Using very simple and easy to break passwords
- Writing down the passwords onto paper

And if the user forgets the password you will have to implement a process where the password can be recovered / reset. E-mail based recovery works adequately in most cases, but sometimes throwaway e-mail addresses are used for registration. An account could have been registered with an e-mail provider that is no longer accessible for the user. Secret questions are difficult to implement properly , and customer service desk phone calls are even more difficult to implement properly .

Password is not strong by any means. Even if the registration process is the most rigorous one in the world, the method itself is too vulnerable.

Online	IoT	PSD2	Convenience	LOA
🟢	🟢	🔴	🟡	🔴



Social Identities

Social identities are handled here as a separate category, even though most of them are based on passwords. The reason is that social identities fall into the category of 3rd party identities. The identity is created and maintained through a 3rd party (the social media site). Some social identities allow you to add an extra layer of security in the form of e.g. one-time-password / code sent to your phone.

For applications social identities provide a convenient way to capture a visitor. Mobile apps, e-commerce sites, forums etc. have been integrating these 3rd party identities and authentication into their applications already for years. For the users it's also very convenient to use their existing identity.

There's no guarantee of the true identity behind a social identity. That makes the social identity somewhat questionable if we want to properly authenticate a user. Social identities are excellent in converting visitors into customers. The identity information is strengthened once the user goes through a transaction where e.g. credit card information is required.

Direct integration to online applications and mobile apps is straightforward through standard protocols, typically OAuth 2.0 or OpenID Connect. For the IoT use case it becomes a question of capabilities - does the device have the relevant protocols supported or hardware capabilities if the user wants to register himself directly with the device.

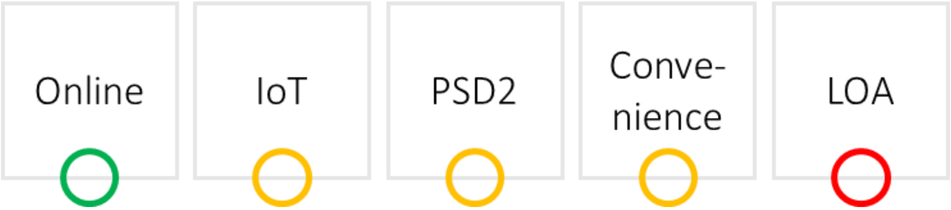
Online	IoT	PSD2	Convenience	LOA
🟢	🟡	🔴	🟢	🔴

Corporate (Business) Identities

Corporate identity (LDAP, Active Directory, Azure AD / O365, Google for Business) is again a mostly password dominated category and handled separately. Corporate issued identities have some advantages over normal consumer or social identity password based systems. If the IT department of the corporation is up for the task, the passwords are usually screened for their strength and the employee is required to change a weak password. A bigger advantage, and higher LoA can be achieved if the company uses a stronger form of authentication, e.g. corporate smart cards.

The identity information of a corporate user can be considered much more reliable than a self-registered account or social identity from the registration point of view. However if the corporate identity is based on passwords, the overall Level of Assurance remains low.

In a business-to-business use case allowing a customer or a partner to single sign-on to your application with their own corporate identity is very convenient and can be seen as a competitive advantage. Another prevalent use case is using the corporate identity to single sign-on to cloud based services. Beyond business-to-business use cases corporate based identities do not offer much.



One-time-passwords

Coming up the ladder on the strength scale we have one-time-passwords. Some of the Scandinavian banks started to issue OTP lists to their customers already in the 90's. Today OTPs can be seen in many forms from these printed OTP lists, SMSs, tokens generating OTPs to mobile apps. There's also a standards on how to generate OTPs.

As the name suggests OTPs are for one-time use. This makes it a stronger alternative compared to passwords. A typical OTP is a string of random numbers (4-8 long). During authentication the user needs to lookup (from the list) or generate an OTP using a token or an app which is then written to the web authentication form. Generated OTPs are usually valid for a short period of time allowing some time for the user to write it to the form and minimizing the possibility of a replay attack later on. Lists are typically used in consecutive order and the list has 30-50 OTPs. SMS based OTPs are sent to the registered mobile phone number of the user.

The convenience of an OTP system is low, perhaps excluding a mobile based method. The fact that the user has to carry the list or specific token with him is a disadvantage. Tokens are also fairly costly for the service provider, especially in the long run as you have to replace them (battery died, broken) or issue a new one (lost token). OTPs are almost always combined with a password, lowering the convenience even further.

On the security front OTPs have a few issues. SMS-based OTPs are no longer recommended by the NIST (link) as e.g. a smart phone malware can capture it, or the gateway used to send the message can be hacked (SS7 vulnerabilities). The other issue is that like the password, the user can by mistake give out the secret. There are several well documented cases where a combination of a good phishing mail with a link to an official looking online site have resulted in hacked accounts protected by OTPs. And these types of attacks are only getting more sophisticated.

Online	IoT	PSD2	Conve-nience	LOA
🟢	🟡	🟡	🔴	🟡

PKI

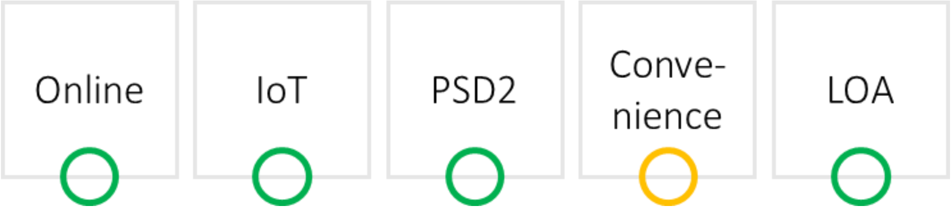
Public Key Infrastructure relies on the very tried and tested algorithm invented already in the 70’s, RSA, and a newer version, ECC (Elliptic Curve Cryptography). The basis is asymmetric cryptography where the user is in a possession of a secret and public key. The public key is verified by a third party (Certificate Authority, CA) and a certificate is issued stating that this public key belongs to this user. The certificate is signed by the secret key of the trusted third party vouching for the authenticity. The notion of the third party is important here as it relates to the registration process and the level of assurance.

PKI or rather certificates come in many shapes and sizes. The trust backbone of the whole Internet is based on certificates and PKI. The green text or the green bar on the browser address field indicates that the online service is using a certificate and communication channel between the service and the browser is encrypted (https). The green bar additionally indicates that the organization using the certificate has been properly vetted when the certificate was issued. So PKI (and certificates) is the technology to identify a service / application to the user in this case.

For the users, certificates are secure alternatives over passwords and OTPs. The secret, the PKI private key, is close to impossible for the end user to hand out to someone else. Typically it never leaves the device where it’s generated. If the organization wishes to implement a key recovery scheme, the private key though needs to be stored somewhere in case the user loses e.g. the device that held the private key.

Software based certificates are very easy to create for example in the operating system level for e.g. a corporate laptop. The downside is that this certificate is tied to the corporate laptop. External devices such as USB-tokens, smart cards or mobile phones as certificate devices are more flexible, mobile phone (SIM card, Trusted Execution Environment or Operating system) perhaps being the most flexible one as it acts as a key generation and storage device and the reader at the same time. For mobile phones we have two main storages where certificates (and the PKI keys) can be saved. The most secure one is the Secure Element (SE) that can be a SIM-card or a Trusted Execution Environment (TEE). SIM cards have the benefit of working in practically all phones. TEE chips are coming more common in modern smart phones. Certificates and keys can be stored also in the operating system level of the mobile device.

Use cases for certificates are too numerous to list here. For authentication, certificate based schemes provide a strength level that should satisfy the requirements of most regulations and standards, especially if the certificate is stored in a secure environment (token, smart card, hardware security module, Secure Element, Trusted Execution Environment). Certificates are also excellent for IoT purposes. They can be used to authenticate both the device and the service the device is talking to – usually a manufacturers' server.



Online ○

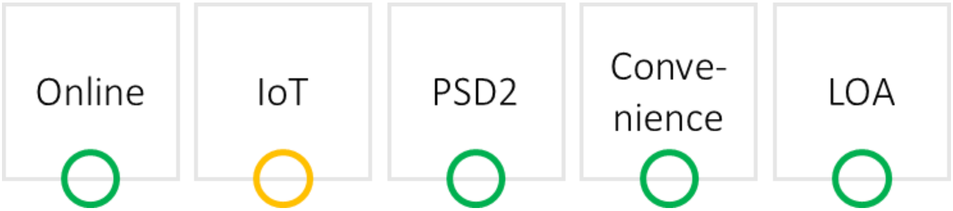
IoT ○

PSD2 ○

Convenience ○

LOA ○

The level of assurance for certificates is normally high, but there are cases where certificates are self-signed, or issued without proper vetting (Paypal example) and the identity behind the private key is really a question mark. The third party mentioned in the beginning of this section, Certificate Authority, provides means to evaluate the registration process and thus the LoA.



Online	IoT	PSD2	Conve-nience	LOA
🟢	🟡	🟢	🟢	🟢

Biometric

The emergence of fingerprint reader equipped smart phones have raised biometrics as one of the most interesting ways how to authenticate a user. Biometrics is a category "something you are". There are plenty of different options for biometrics starting with the fingerprint to eye to even behaviour. If it can be measured and a template can be created for comparing purposes, it can be used as a biometric identifier.

The best part of the biometric authentication method is in the usability. If the biometric authentication scheme can leverage e.g. the fingerprint reader on a modern smart phone, it outshines all the other methods in convenience. Other, perhaps more obscure, methods can have questionable convenience, but the proliferation of smart phones with biometric capabilities should ensure that they are the main devices where biometric authentication will be implemented.

Biometric authentication can be implemented in two different ways. The biometric –only and using biometric authentication in combination of another technology. Relying solely on biometric authentication is much more complex effort and can result into biometric database breaches as the templates need to be stored somewhere centrally. Another downside of a biometric factor is that it's hard to change. There are technologies that can be used such as cancellable biometrics to enable template changes in case the existing one is compromised.

The best way to deploy biometric authentication is to use the biometric factor to unlock another secret. Instead of using the PIN protecting the PKI private key on a phone we can use the smartphone fingerprint reader. In essence it's about replacing "something you know" with "something you are" giving you at least 2-factor authentication. If you start the whole process with a password ("something you know") you have a fairly convenient multi-factor authentication at your disposal. The overall LoA score depends highly on the registration process.

Multi-factor Authentication

Multi-factor authentication means that more than one factor is used to verify the identity. The main categories of these factors are

- Something that you know (password, PIN code, answer to a secret question)
- Something that you have (token, smart card, phone)
- Something that you are (fingerprint, eye, blood vessel pattern, heartbeat, DNA, behaviour)

By combining these factors we get a multi-factor authentication scheme. Multi-factor does not automatically mean that you have a strong authentication method. A good multi-factor authentication integrates at least one strong factor (PKI, biometrics) into the method. In some markets OTP is considered a strong factor, and it definitely strengthens the authentication scheme

Online	IoT	PSD2	Conve- nience	LOA
🟢	🟡	🟢	🟡	🟢

Online	IoT	PSD2	Convenience	LOA
🟢	🟡	🟢	🟢	🟢

Mobile

We have touched mobile based authentication methods in the previous chapters. The modern smart phone is an excellent device where to implement a second and/or third factor into the authentication process. Feature phones can also work in the authentication scheme, but the options are much more limited as the user can’t add new apps to the phone.

Besides PKI and biometrics smart phones have dozens of authentication apps in the marketplace. An easy to use and convenient way to add “something that you have” factor to the authentication is to simply require the user to tap/swipe the phone app indicating that he’s in the possession of the device. OTP generator apps are very common for smartphones, and both feature and smartphones can be used to receive SMS based OTPs.

When we use a mobile device and implement the biometric factor in the authentication, it needs to be done properly. Select iOS and Android devices have the capability to scan the fingerprint of the user and their cameras can be used to implement facial recognition, or even iris scanning. The appropriate way to utilize the biometric factor is to replace a secret protecting a PKI private key within the app. In a traditional PKI method the private key is protected by a PIN code (smart cards, PKI tokens, mobile PKI). Even the tap/swipe “Ok” can be used to unlock the private key, but then the LoA should be considered to have a lower value as it is still only proof of possession. With biometrics you have both the proof of possession and the “something that you are” factors.

If you start the authentication process by writing your phone number and a password to the online form and then proceed to mobile based biometric authentication, you have covered all 3 main factors in your authentication scheme (know, have, are). The mobile based authentication can offer you one of the strongest schemes in the market that is also extremely convenient for the end user. If the registration of the identity is done properly it offers one of the best LoAs in the market, only perhaps superseded by PKI smart cards.

Quantum Key Distribution (QKD)

For the most secure systems Quantum Key Distribution offers the strongest alternative in existence. QKD is a method of exchanging encryption keys by relying on quantum mechanics and detection of photons and at this point in time provides the ultimate in secrecy. QKD is not intended for end user authentication. It’s currently used in securing point-to-point connections between servers that require the utmost security. Currently there are no viable methods how to breach QKD itself.

QKD is perhaps an example of coming technologies. As with any other technology, information security is a constantly evolving field. QKD is not quantum computing. The arrival of quantum computing will certainly bring a new set of possibilities and challenges along with it.

Online	IoT	PSD2	Convenience	LOA
🟢	🔴	🟢	🔴	🟢

Step-up Authentication and benefit of appropriate authentication

When we consider what type of authentication method should be used, we must first evaluate how confidential the target resource is, and who is the intended audience. Terms like weak authentication or strong multi-factor authentication are meaningless without this context. A much more suitable term would be “appropriate authentication”. The application should use an appropriate authentication method that reflects the confidentiality level of the data within the application.

If we consider the simple example given in the beginning of this paper, we can extend it a bit. Let’s assume that two of the applications behind the front-end have data at a low level of confidentiality. For the provider it would suffice if they can determine if the user has registered and used the service before. For this purpose a weak authentication method such as a password or social identity is enough. However, the other two applications hold much more confidential data within them.

Step-up authentication is a process that forces the user to authenticate themselves using a higher LoA identity. This is a very useful technology as it allows the service provider deploy weaker, cheaper and more prevalent authentication methods to capture the visitor, and at the same time protect the confidential data within other applications through stronger authentication requirements.

Integration

Perhaps beside the password method, other authentication methods need to be integrated to the applications. You can purchase authentication solutions separately but then you end up in a situation where you might have different solutions from different vendors using different protocols. The result is a complex environment with high management overhead and you might create security gaps inadvertently. It might also result into separate identity silos which will make complying to regulation more difficult (EU, GDPR).

The best option to avoid this kind of situation is to deploy an identity provider (IdP). The IdP forms a link between the applications and authentication solutions. It also allows you to use third party authentication sources such as social media, bank, mobile network operator (Mobile Connect) identities or even government issued strong identities all through the same solution. A good IdP also supports the application protocols for authentication making it easy to deploy multiple different authentication solutions for the applications.

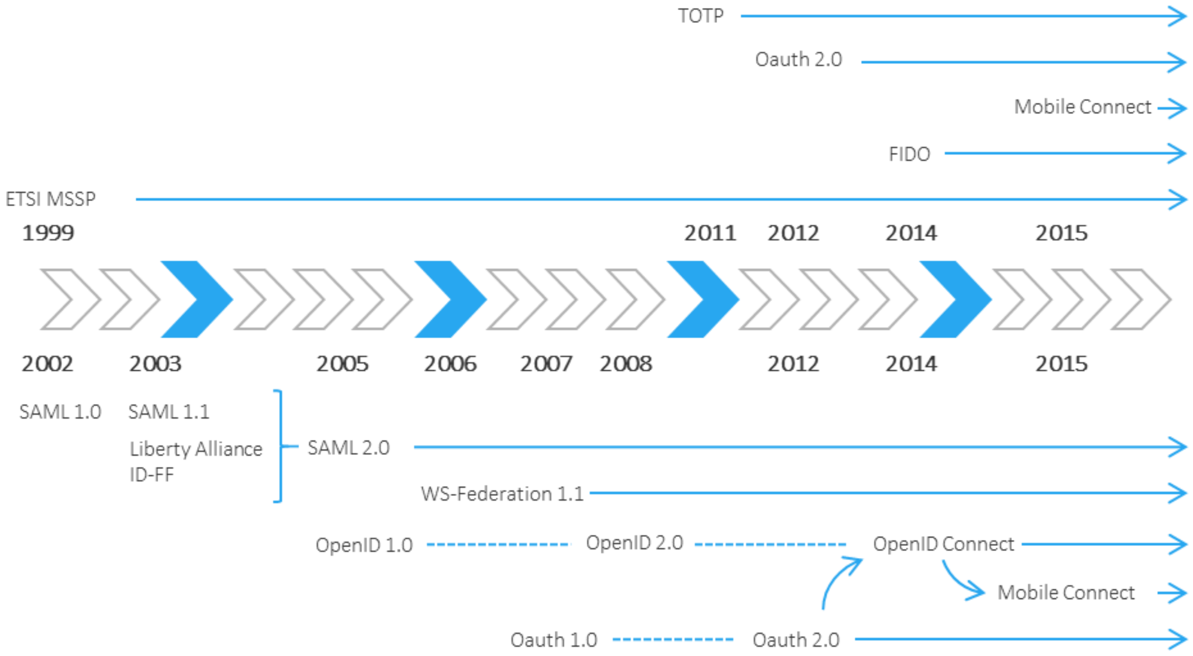
Another advantage of an IdP is Single Sign-On. Once the user has been authenticated into one application, he can move between the applications without re-authentication. If the initial authentication was done using a lower level of assurance method, step-up authentication is required to access the more confidential areas, and the IdP can take care of this using visually the same kind of login flow. If the user first authenticated with a higher level of assurance method, moving to resources that require lower level of assurance methods will not trigger a new authentication request.

Identity Provider also takes care of sending the correct identity attributes to the applications along with the authentication information. This will ensure that each and every application only receives the information it actually needs about the user, nothing more. This kind of functionality is reflected in e.g. the new European regulation; General Data Protection Regulation (GDPR).

Protocols

Web Single Sign-On is not a new phenomenon. Standards for Single Sign-On solutions started already over a decade ago. As time has passed some standards have merged and new ones have been created. SAML (Security Assertion Markup Language) is one of the oldest Web SSO protocols and it has a strong foothold in the field, especially in the e-government services. WS-Federation was in the beginning mainly a Microsoft developed standard that has now found its way into other products as well. The modern cloud services, IoT and mobile apps have created a demand for simpler Web SSO protocols and OpenID, OpenID Connect, OAuth and Mobile Connect have emerged.

For the service provider who is running more than one application the ability to integrate various authentication options becomes important. It's also good to review how omni-channel strategies will be affected, or what kind of authentication is needed depending on the channel the end users are using. An Identity Provider is again a tool to simplify the integration process and allows companies to deploy e.g. smart phone apps that do not require a new version in the app store if authentication requirements change.



Policy Control Point

Authentication is a process of validating claims or assertions that the visitor presents in order to establish an identity. Authentication decisions are binary. Either the user can access the application or not. The decision about the access can be made in two places. We can build the logic into the application or we can use a centralized solution where the access decisions are handled.

The logic on how to establish the identity is called a policy. A very simple authentication policy would be to check the password from the web form against the password stored in the database. When we move towards more complex policies and include dynamic group member information, attributes of the user etc. we are actually talking about an authorization policy. However, the end result will be the same; the user is granted or denied access.

A simple policy is easy to build within the application. Though there are immediate drawbacks even with simple policies. Each application need to be maintained separately, and in most cases the result can be multiple independent identity repositories making it harder to comply e.g. GDPR requirements of “right for erasure” and data portability. If the policies become more complex, the maintenance becomes a headache and can result into security gaps due to poor coordination between different applications.

A centralized policy control point implemented by e.g. an Identity Provider (IdP) creates a much more flexible and secure environment. A proper IdP can be integrated to multiple different application platforms using different standards. It can also link to external identity sources such as social media, bank IDs, mobile network operator IDs or government issued eIDs.

Summary

Different authentication mechanisms have different strengths in the registration process, resistance to discovery / breach, how they either enable you to increase revenue by reducing friction or allow the creation of new digital services through better KYC or security. The Payment Service Directive 2 is driving the financial industry to adopt strong customer authentication, and we've tried to cover which authentication categories are worth investigating if your organisation is affected by the directive. However, please note that the Regulatory Technical Standard for Strong Customer Authentication does not outline any specific technologies when it comes to PSD2 compliant mechanisms. And the PSD2 is a directive, therefore local implementations by Member States might have an effect on authentication.

A good online service offers not just one, but 2 or more different authentication methods, or categories. Weak methods are good for capturing visitors, but anything involving transactions should increase the authentication method strength. So, depending on the nature of your services you might need multiple social media methods, and if transactions are conducted, (a) stronger method(s) to implement KYC and confirm transactions. At the stronger end of the scale, both for method strength and registration process, you'll find government issued PKI smart cards. An Identity Provider (IdP) is a tool that allows you to quickly integrate these methods to your services using standard protocols. IdPs support different methods and categories, and by investigating which methods are supported you should be able to find a suitable Identity Provider for your organisation.

	Online	IoT	PSD2	Convenience	LOA
Passwords	🟢	🟢	🔴	🟡	🔴
Social Identities	🟢	🟡	🔴	🟢	🔴
Corporate (Business) Identities	🟢	🟡	🟡	🟡	🔴
One-time-passwords	🟢	🟡	🟡	🔴	🟡
PKI	🟢	🟢	🟢	🟡	🟢
Biometrics	🟢	🟡	🟢	🟢	🟢
Multi-factor Authentication	🟢	🟡	🟢	🟡	🟢
Mobile	🟢	🟡	🟢	🟢	🟢
Quantum Key Distribution (QKD)	🟢	🔴	🟢	🔴	🟢

UBISECURE™

“

THERE ARE BILLIONS OF ONLINE AND MOBILE IDENTITIES AND THEY EXIST IN FRAGMENTED DOMAINS, SEPARATE ECOSYSTEMS DESIGNED FOR INDIVIDUAL PURPOSES.

WE SEE A WORLD OF DIGITAL TRANSFORMATION DRIVEN BY THE NEED FOR CUSTOMER/USER SERVICE. KEY TO THAT PROCESS ARE THE TENANTS OF SECURITY AND SIMPLICITY. SERVICE PROVIDERS ARE LOOKING TO EVOLVE, EMBRACE AND EMPOWER THEIR USERS, AND IN DOING SO INCREASE THE EFFICIENCY AND PROFITABILITY OF THEIR CUSTOMERS.

THE ABILITY TO OUTSOURCE IDENTITY, LEVERAGE THE SECURITY OF PROVEN PLAYERS, AUTOMATE THE MAINTENANCE AND ONBOARDING OF NEW IDENTITIES IS KEY TO THE EFFICIENT AND COST EFFECTIVE IMPLEMENTATION OF A DIGITAL TRANSFORMATION STRATEGY.

UBISECURE HAS PROVEN CAPABILITIES TO PUT IDENTITY AT THE BEGINNING OF EVERY DIGITAL TRANSFORMATION.

Simon Wood

Group CEO, Ubisecure

UBISECURE™

ABOUT UBISECURE

Ubisecure is a global Identity & Access Management software and cloud services provider. Ubisecure technology makes using online identities easier, safer and more private for consumers. It helps businesses improve user experience and reduce costs through increased customer engagement, loyalty and insight and it helps service providers benefit from simplified registration, login and attribute sharing from the rich identities already being used online. It helps create trusted connections be-tween digital services, devices and mobile identity. When these modern aspects of identity management are combined, Ubisecure enables the true potential of digital business. The company headquartered in Finland works through a network of local and global system integrator partners and has offices in the UK.

CONTACT US

www.ubisecure.com
sales@ubisecure.com

Tekniikantie 14
02150 Espoo
Finland

The Granary, Hermitage Court
Hermitage Lane, Maidstone
Kent, ME16 9NT, UK