Identity Management

A visual guide to identity verification and authentication for service design in government

hippodigital

The Identity Management Process

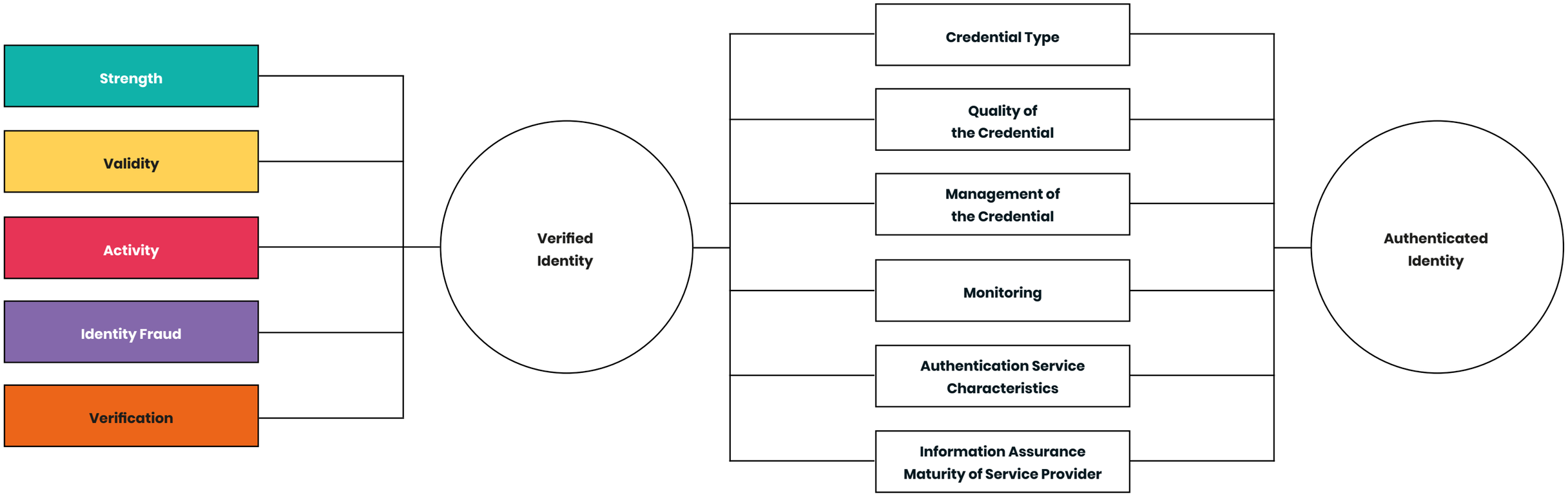
Presented here is a diagram of how identity verification and authentication feed into one another. Although the two processes are linked, they can also occur independently of one another.

Identity Verification

Identity verification is the process of verifying an individual's "claimed identity": the combination of information (e.g name, date of birth etc.) about whoever a user is claiming to be.

Identity Authentication

Authentication (logging-in) is a method for accessing services. When linked with a verified identity it gives the service a level of confidence of who the user is so that we can find out whether they can access a service or not.



Identity verification

Identity verification

Identity verification is the process of verifying an individual's "claimed identity:" the combination of information (e.g name, date of birth etc.) about whoever a user is claiming to be.

The Building Blocks of Identity

We evaluate five elements when verifying an individual's claimed identity. These can be seen as building blocks that allow us to piece together an individual's claimed identity.

Strength

check the strength of the evidence presented in support of a claimed identity, i.e. how hard it is to forge or counterfeit or tamper, and how hard it is for an individual to obtain it.

Validity

check if the evidence presented in support of a claimed identity is either genuine (i.e. not counterfeit), valid (i.e. not expired or cancelled), or both.

Activity

check if the claimed identity has existed over time and has activity associated with it in the form of trusted interactions like credit card transactions, and/or trusted records, like employment records

Identity Fraud

check if the claimed identity is at a high risk of identity fraud. You can do this by checking the details of the claimed identity with authoritative counter-fraud data sources.

Verification

check that the claimed identity belongs to the person who is claiming it through assessing a combination of knowledge-based verification challenges and biometric information.

Identity verification

Identity verification is the process of verifying an individual's "claimed identity:" the combination of information (e.g name, date of birth etc.) about whoever a user is claiming to be.

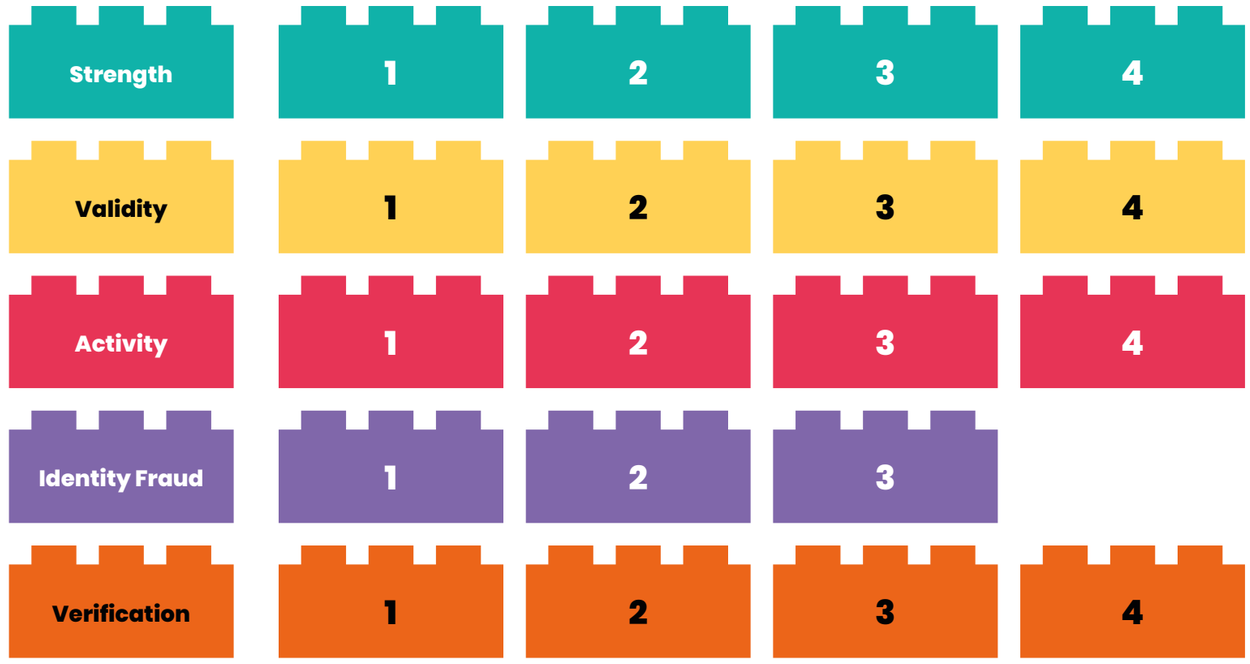
So, how do we verify an identity?

Each identity element / building block has a different level at which we can evalaute it, denoted by score values. Pictured alongside are the five identity elements / building blocks and the respective scores we can assign to them. Bar identity fraud, which is scored on a 3-point-scale, the highest score an element can receive is 4.

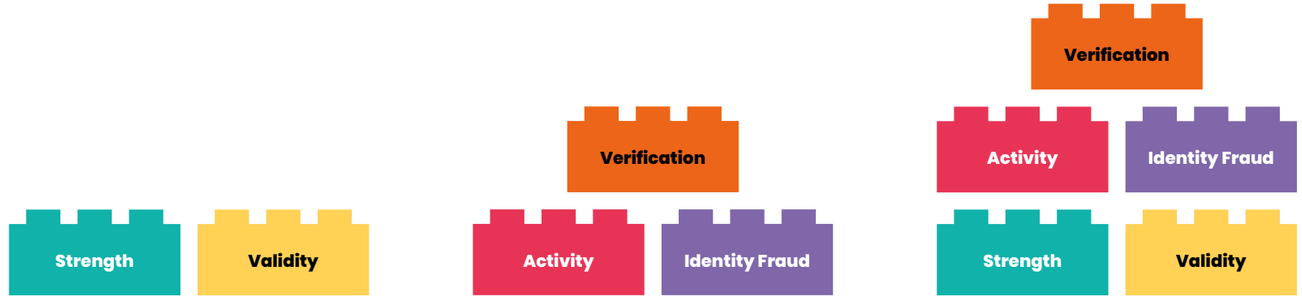
In using these building blocks to verify an identity, we:

- begin by evaluating the strength and validity of each piece of evidence presented in support of a claimed identity. Each piece of evidence receives its own distinct strength and validity score.
- once we know that strong and valid evidence has been presented in support of a claimed identity, we can proceed to evaluate the claimed identity's activity, its risk of identity fraud, and to verify that the claimed identity truly belongs to the person claiming it.

The elements and their score values



The process of verifying an identity



Step 1: Begin by evaluating the strength and validity of each piece of evidence presented in support of a claimed identity.

Step 2: Proceed to build on this to verify the claimed identity's activity, risk of identity fraud, and to verify that the claimed identity belongs to the person claiming it.

Step 3: Bringing all of this together allows us to verify an identity.

Scoring the elements

Defined below are the metrics we use to assign a score to strength of the evidence presented in support of a claimed identity.

Strength

Score	1	2	3	4
Criteria	The evidence will have a score of 1 if it has **at least** two of the following: • the claimed identity's name • the claimed identity's date of birth • the claimed identity's place of birth • the claimed identity's address • the claimed identity's biometric information • a photo of the claimed identity • a reference number The evidence should come from an organisation that: • will check the person's identity when they issue the evidence • ensure its process for issuing the evidence will not be misused by people associated with the organisation. **Examples of evidence that meet a strength score of 1:** • E-mail, PDF, or letter from a local authority.	The evidence will have a score of 2 if it has everything it needs to get a score of 1 and includes information that's unique to either: • the identity • that piece of evidence It also: • shows the person's name instead of any pseudonyms, aliases or nicknames (if the evidence includes a name). • is protected by physical security features that stop it from being reproduced without specialist knowledge or information (if the evidence is a physical document). • is protected by cryptographic security features that can correctly identify the organisation that issued it (if the evidence includes digital information). **Examples of evidence that meet a strength score of 2:** • Birth Certificate • Bus Pass • Education certificate like an A-Level degree certificate	The evidence will have a score of 3 if it has everything it needs to get a score of 2 and: • it includes information that's unique to both the identity and that piece of evidence • the organisation that issued the evidence made sure it was received by the same person who applied for it • the organisation that issued the evidence checked the person's identity in accordance with the 2017 Money Laundering Regulations It must also: • show the person's 'official' name, instead of their initials or synonyms (if the evidence includes a name). • be protected by physical security features that stop it from being reproduced without specialist equipment (if the evidence is a physical document) The evidence must also include one of the following: • a photo of the person • biometric information that uses cryptographic security features • cryptographic security features that can identify the person (including evidence with cryptographic chips & secure digital accounts protected by cryptographic methods). **Examples of evidence that meet a strength score of 3:** • UK driving licences / bank accounts	The evidence will have a score of 4 if it has everything it needs to get a score of 3 and: • it includes biometric information • all digital information (including biometric information) is protected by cryptographic security features which can be linked to the issuing organization • the organisation that issued the evidence proved the person's identity by comparing and matching the person to an image of the claimed identity from an authoritative source **Examples of evidence that meet a strength score of 4:** • UK biometric residence permit • Passports

Scoring the elements

Defined below are the metrics we use to assign a score to the validity of the evidence presented in support of a claimed identity.

Validity

Score	1	2	3	4

Criteria	The evidence will have a score of 1 if the physical features of the evidence appear to be genuine, which can be evaluated by checking that:
	• an original, certified copy or scan of the evidence is being verified
	• there are no errors on the evidence, like wrong paper type, spelling mistakes, irregular use of fonts or missing pages
	• the details, layout or alignment of the evidence look the way they should
	• Any logos look the way they should
	• Any references to information are the same across the evidence (for example if the body text of a letter references an address, this should match the address shown at the top of the letter)
		The evidence will have a score of 2 if we can do one of the following:
		• Confirm the evidence is valid by comparing it to information held by an authoritative source, i.e. a source that maintains the integrity of information about an identity, like the Home Office.
		• Confirm, using a trained checker or certified system, that the visible security features are genuine (these are security features that can be seen without using specialist light sources). To do this:
		  • you cannot accept photos scanned versions of the evidence
		  • you need to make sure the evidence has not expired
		  • you need to ensure that the evidence was delivered to you securely
		• Confirm, using a trained checker or certified system, that the ultraviolet (UV) or infrared (IR) security features on the physical evidence are genuine.
			The evidence will have a score of 3 if we can do all of the things listed as requirements for a validity score of 2, as opposed to only doing one of them.
			To achieve a score of 3, we also examine the visible security features and UV and IR security features of a piece of evidence with further scrutiny than what is required at level 2. In particular, we ensure the evidence has not been re-used and that all the security features adhere to the latest official template for a particular piece of evidence.
			Alternatively, we can check whether the cryptographic security features associated with the pieces of evidence provided are genuine. We can do this by:
			• making sure the evidence has not expired.
			• reading the cryptographically-protected information.
			• providing required cryptographic keys.
			• checking the digital signature is correct.
			• checking the signing key belongs to the organisation that issued the evidence and that it is the correct type of key for that evidence.
			• checking the signing key has not been revoked.
				The evidence will have a score of 4 if you can do all of the following:
				• Confirm the visible security features meet the criteria required for score 3, but do this under the supervision of another trained checker and under controlled conditions.
				• Confirm the UV or IR security features meet the criteria required for score 3
				• Confirm the cryptographic security features meet the criteria required for score 3
				• Check to make sure the evidence has not been cancelled by the organisation that issued it. You can do this by checking an authoritative database of cancelled evidence, for example Interpol for passports or a mobile phone operator for mobile phone contracts.

Scoring the elements

Defined below are the metrics we use to assign a score to whether the claimed identity has existed over time and whether it has activity associated with it.

Activity

Score	1	2	3	4
Criteria	The evidence will have a score of 1 if you: • Have evidence of interactions between the claimed identity and an organisation • Know the organisation checked the claimed identity is who they say they are • These interactions need to have happened over the last year and in a way that you'd expect the claimed identity to behave	The evidence will have a score of 2 if you: • Have evidence of interactions between the claimed identity and an organisation • Know the organisation used an authoritative source to check the claimed identity was who they said they were • These interactions need to have happened over the last 6 months and in a way that you'd expect the claimed identity to behave	The evidence will have a score of 3 if you: • Have evidence of interactions between the claimed identity and an organisation • Know the organisation checked the claimed identity was who they said they were in a way that at least met the requirements of the Money Laundering Regulations 2017 • These interactions need to have happened over the last 3 months and in a way that you'd expect the claimed identity to behave	The evidence will have a score of 4 if you: • Have evidence of interactions between a claimed identity and an organisation • Know the organisation checked the claimed identity was who they said they were in a way that at least met the requirements of the Money Laundering Regulations 2017 • Know the organisation compared the claimed identity to an image from an authoritative source • You'll need to find at least one interaction from the last 3 months.

Scoring the elements

Defined below are the metrics we use to assign a score to the claimed identity's risk of identity fraud.

Identity Fraud

Score	1	2	3
Criteria	You'll get a score of 1 if you use an authoritative source to check if the claimed identity has either: • had its details stolen (even if those details have not been used fraudulently yet) • been reported as stolen • If either of these things have happened, you must conduct extra verification checks. • You must also use an authoritative source to check if the claimed identity is a known synthetic identity. If it is, you must reduce these risks by: • doing additional verification checks • collecting more evidence of the claimed identity	To get a score of 2 you must do all the checks needed to get a score of 1. You must also use an authoritative source to check that the claimed identity: • belongs to someone who's still alive • is known by an organisation that should have a record of that person (for example an Electoral Registration Office in a local authority) • is at a usual risk of being impersonated (for example, a 'politically exposed person' like a politician or judge is at a higher than usual risk of being impersonated). • You must do extra 'verification' checks if any of these things do not apply.	You'll get a score of 3 if you use more than one authoritative source to do all the checks needed to get a score of 2. Further, the sources must also be 'independent', which means they're either: • separate from the part of your organisation that checks identity • part of a different organisation

Scoring the elements

Defined below are the metrics we use to evaluate whether a claimed identity belongs to the person who is claiming it.

Verification

Score	1	2	3	4

Criteria	The person will get a score of 1 if they can give you information that does not change over time ('static' information) that only the claimed identity should know.
	
	You should check this by asking the person to answer questions or complete tasks. These are known as 'knowledge-based verification' (KBV) challenges.
	
	You should ask the person to do one of the following:
	• 2 low quality KBV challenges
	• 4 low quality multiple choice KBV challenges
	• 1 medium quality KBV challenge
	• 2 medium quality multiple choice KBV challenges
	• 1 high quality KBV challenge
		The person will get a score of 2 if you do one of the following:
		• Make sure the person physically matches the photo on or associated with the strongest piece of genuine evidence you have of the claimed identity (in person or remotely).
		• Make sure the person's biometric information matches biometric information from the strongest piece of genuine evidence you have of the claimed identity.
		• You must ensure the biometric information hasn't been tampered with, isn't being reused, is being presented by a real person, and that your system is secure enough to verify it.
		• Ask the person to complete multiple 'dynamic' KBV challenges (i.e. challenges with answers that change over time) that only the claimed identity should be able to do. You should ask the person to complete the following:
		  • 4 low quality KBV challenges
		  • 8 low quality multiple choice KBV challenges
		  • 2 medium quality KBV challenges
		  • 3 medium quality multiple choice KBV challenges
		  • 2 high quality KBV challenges
		  • 2 high quality multiple choice KBV challenges
			The person will get a score of 3 if you do either of the following in person or remotely:
			• make sure they physically match the photo on (or associated with) the strongest piece of genuine evidence you have of the claimed identity.
			• make sure their biometric information matches biometric information from the strongest piece of genuine evidence you have of the claimed identity at a level that meets score 2 criteria, and:
			  • your system's security is aligned to industry best practice standards like ISO/IEC TR 29156:2015.
			  • your system's biometric algorithm is aligned to a recognised benchmark like the NIST's guidance on facial recognition.
			  • the biometric information is verified under controlled conditions
			  • your system takes multiple steps to ensure that the biometric information is being presented by a real person (for example, NHS Login has users send a video to match them to their biometric data and ensure that they are real people).
				The person will get a score of 4 if:
				• you make sure their biometric information matches biometric information from (or associated with) the strongest piece of genuine evidence you have.
				• All criteria for biometric information at score 3 are met, and the system also ensures that extensive protections are in place to prevent advanced identity fraud methods that take a significant amount of resources to create, like deep-fakes.

Identity Profiles

Identity profiles can essentially be seen as templates against which we can verify individual's claimed identities, and which we can choose based on the level of confidence at which a service needs to verify its users.

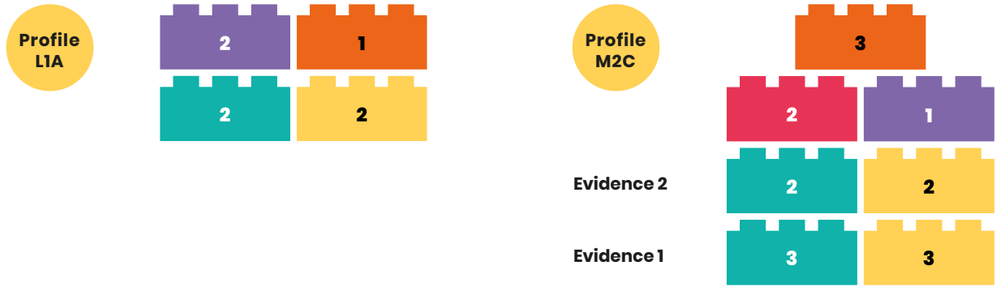
Building Identity Profiles

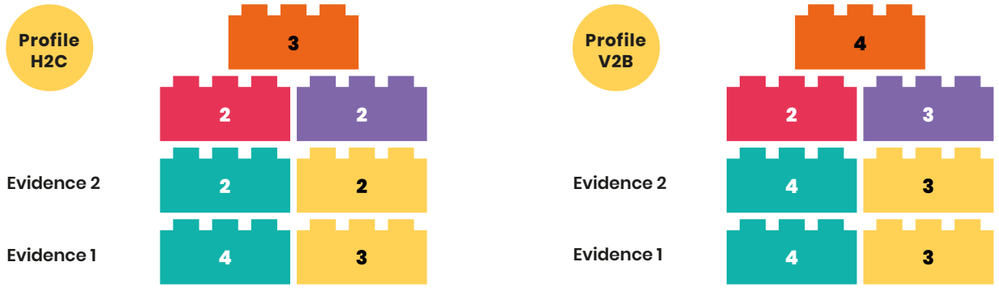
Different combinations of these five building blocks at the different score values explored above allow us to build a wide range of identity profiles. In turn, identity profiles can broadly be grouped into four levels:

- Low Confidence Identity Profiles
- Medium Confidence Identity Profiles
- High Confidence Identity Profiles
- Very High Confidence Identity Profiles

We choose different profiles based on the level of assurance at which a service needs to verify users. The diagrams alongside demonstrate how these building blocks can come together to build a wide range of identity profiles.

For Example





Presented above are a few examples of how the building blocks at their respective score values can come together to form a wide range of identity profiles at varying levels of confidence, from low-confidence identity profiles through to very-high-confidence identity profiles.

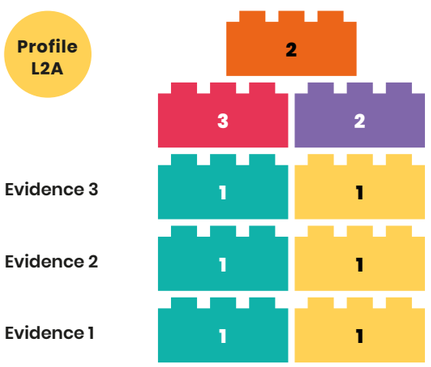
To demonstrate, to build profile M2C, we need the first piece of evidence to be at a strength and validity score of 3 and the second piece of evidence to be at a strength and validity score of 2. Once we have scored the strength and validity of the evidence presented in support of the claimed identity, we can score the other building blocks required to build profile M2C. To meet the requirements for profile M2C, we need to ensure that the claimed identity's risk of identity fraud is at a score of 1, the claimed identity's activity is at a score of 3, and verify that the claimed identity belongs to the person claiming it to a verification score of 3.

Low confidence identity profiles

We use low confidence identity profiles if our service lets users view or update personal information.

With 1 piece of evidence, we can build 3 low confidence identity profiles

With 3 pieces of evidence, we can build 1 low confidence identity profile



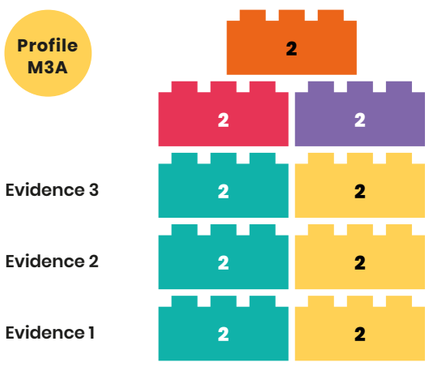
Medium confidence identity profiles

We use medium confidence identity profiles if our service gives users access to sensitive information, money or benefits.

With 1 piece of evidence, we can build 2 medium confidence identity profiles

With 2 pieces of evidence, we can build 4 medium confidence identity profiles

With 3 pieces of evidence, we can build 1 medium confidence identity profile



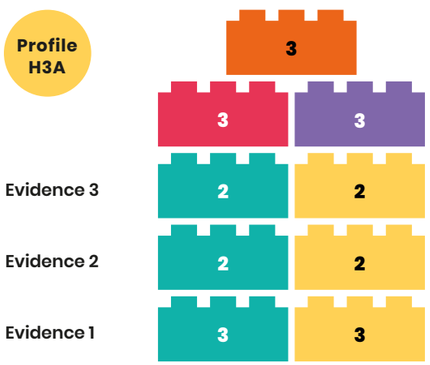
High confidence identity profiles

We use high confidence identity profiles if our service gives users access to secure buildings, like nuclear power stations, or highly secure information, like classified government documents.

With 1 piece of evidence, we can build 2 high confidence identity profiles

With 2 pieces of evidence, we can build 3 high confidence identity profiles

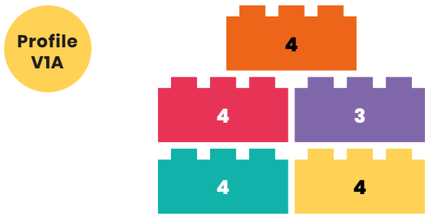
With 3 pieces of evidence, we can build 1 high confidence identity profile



Very high confidence identity profiles

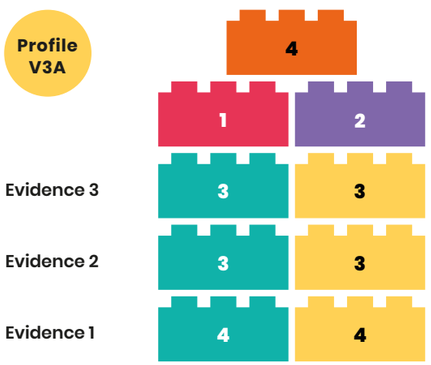
We use very high confidence identity profiles if our service gives users access to secure buildings, like nuclear power stations, or highly secure information, like classified government documents.

With 1 piece of evidence, we can build 1 very high confidence identity profile



With 2 pieces of evidence, we can build 2 very high confidence identity profiles

With 3 pieces of evidence, we can build 1 very high confidence identity profile



Authentication

Authentication

Authentication (logging-in) is a method for accessing services. When linked with an identity it gives the service a level of confidence of who the user is so that we can find out whether they can access a service or not.

Level 1

We are verifying whether a user engaging with a service / system is in possession of a legitimate credential.

We are not verifying whether the credential is being used by its owner, exposing the owner to the risk of credential theft.

e.g.: a given user can enter a password that may or may not belong to them.

Level 2

We are verifying whether a user engaging with a service / system is in possession of a legitimate credential.

We are also checking whether said user is the owner of said credential, or has the owner's explicit consent to use their credential. This protects the owner from credential theft.

e.g.: when a firm asks you to use two-factor authentication on your phone to prove your identity

Level 3

We are verifying whether a person engaging with a service / system is in possession of a legitimate credential.

We are also checking whether said user is the owner of said credential, or has the owner's explicit consent to use their credential. This protects the owner from credential theft.

We are also able to protect the user from attacks where the credential has been compromised.

e.g.: when you get an e-mail from Gmail if someone logs in to your account from a different device, and - if that someone isn't you - gives you options to recover your account.

Credential Characteristics

We authenticate a claimed identity based on 6 credential characteristics; these are scored using the three authentication levels listed previously. These characteristics evaluate the credentials used to authenticate a claimed identity.

Credential Type

A complex credential is much harder for an attacker to guess. When verifying identity, a set of credentials applies to each authentication level.

Level 1 Criteria
The user uses a credential that demonstrates they possess a secret, like a password or a PIN number, belonging to the owner.

Level 2 Criteria
The user uses a credential that demonstrates they possess a secret belonging to the owner, shared over a channel separate to the authentication channel. Plus, the user possesses a credential that is linked to the owner's biometric details, e.g. a fingerprint.

Level 3 Criteria
The user uses a credential that demonstrates they possess a hardware token (YUBI key) or software token (two-factor authentication by phone) that belongs to the owner.

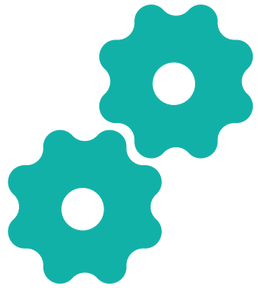
Quality of the Credential

Using metrics to verify the quality of a credential when authenticating someone's identity. Here, we are evaluating the measures a credential takes to ensure that it isn't compromised in any way.

Level 1 Criteria
The credential contains no measures to prevent duplication, but the user is encouraged to use secure credentials (e.g. users are guided to pick passwords with a mix of numbers, letters, and symbols).

Level 2 Criteria
The credential has measures to prevent duplication and prediction. The credential has measures to prevent tampering and uses industry-standard hardware and software tokens. The credential uses cryptographic modules that meet good industry practice standards.

Level 3 Criteria
The credential has level 3 measures that prevent compromise from tampering and has measures to prevent duplication and prediction. The credential uses cryptographic modules that meet good industry practice standards.



Management of the Credential

How the identity provider manages a given user's identity and the processes they use to ensure secure identity management.

Level 1 Criteria
The authentication provider must take steps to ensure credentials are delivered to their owner. The authentication provider should be able to suspend and / or revoke a credential with immediate effect. Manufactured / generated credentials must be subject to quality management & data transfer needs to be highly secure. All credentials must be protected from physical and electronic theft / damage & the user should be able to recover & request new credentials. Only the user must be allowed to make changes to their credentials.

Level 2 Criteria
All criteria for Level 1 must be met, & reasonable steps must be taken to ensure credentials are delivered to owners. Credential manufacturers must have independently audited quality and information management systems.

Level 3 Criteria
All Criteria for Level 1 and 2 must be met, & all reasonable steps must be taken to ensure credentials are delivered to owners. Credential manufacturers must have independently certified quality and information management systems.

Credential Characteristics

We authenticate a claimed identity based on 6 credential characteristics; these are scored using the three authentication levels listed above. These characteristics evaluate the credentials used to authenticate a claimed identity.

Monitoring

Evaluating whether the identity provider has taken steps to ensure that given credential is not being misused.

Level 1 Criteria
Authentication provider monitors credential activity. If there is reasonable suspicion that the Credential is being used by someone other than its owner, the authentication provider shall take measures to determine the user is the owner of the Credential; this may include revoking and replacing the Credential. (e.g.: cancelling a credit card after suspicious behavior has been identified).

Level 2 Criteria
All criteria for level 1 are met. The authentication provider creates benchmarks of normal behaviour to better identify abnormal behaviour. Abnormal behaviour must be reported.

Level 3 Criteria
All criteria for level 1 and 2 are met. The authentication provider shall check Her Majesty's Government provided services for indications that the credential may be hijacked.

Authentication Service Characteristics

The Authentication Service must protect the user and itself from compromise. Certain criteria can be used to benchmark whether a service successfully achieves this.

Level 1 Criteria
The authentication service only returns a success when the user has successfully authenticated using their credential., and rejects otherwise. Authentication sessions must be protected by Good Industry Practice measures, and any cryptography used must meet Good Industry Practice standards.

Level 2 Criteria
All criteria for Level 1 are met. The authentication provider shall take measures to ensure that non-human operators cannot use a user's credentials. Measures like 2-factor authentication must be in place to prevent replay of credentials. Measures exist to protect credential from compromise, even if communication channel is compromised.

Level 3 Criteria
All criteria for Level 1 and 2 are met. The Authentication provider shall take measures to both detect and prevent the illegitimate use of a user's credentials.

Information Assurance Maturity

A measure of how advanced and competent an Authentication Provider's information security and management processes and systems are.

Level 1 Criteria
The authentication provider has an effective information security management system, including a forensic readiness plan, an audit regime, and an internal monitoring regime covering all systems supporting the use of the credential. All systems supporting the use of the credential must also have a consistent time. Further, a monitoring regime should be in place to detect undesirable activity within the service, and regular risk assessments must be conducted with defined processess for exception handling. Lastly, the authentication provider must have a records management system covering all systems supporting the credential.

Level 2 Criteria
All Level 1 criteria must be met and subject to scrutiny by an independent auditing body. The authentication provider shall test its monitoring regime through a schedule of independent vulnerability and penetration tests, adjusting it to address any issues discovered.

Level 3 Criteria
All Level 1 and 2 criteria are met and the authentication provider is subject to independently certified information systems, audit regimes and record management systems. System times must be synchronized to a Stratum 1 Time Source.

Recommended Further Reading

The following document is a summary of information contained within GOV UK's GPG 44 and GPG 45 guidelines on identity verification and authentication respectively. For further information and to dig into identity verification and authencitation further, we recommend you refer to these documents via the following links:

GPG 44: Authentication and Credentials for use with HMG Online Services

GPG 45: Identity Proofing and Verification of an Individual

About Hippo Digital

What we do

We seek to design and build services that improve people's lives.

Service Design

We design evidence-based, people-centred services that meet the intended outcomes of our clients. We work awith our clients by becoming part of the team, usually on site.

Build

We integrate lean people-centred design with Agile delivery and DevOps. Our iterative, rapid, data-driven design and build allows us to consist-ently deliver meaningful outcomes.

Customer Experience

We deliver personalised customer experiences. This improves relationships between organisations and their customers, and makes it easier for people to do what they need to do.

Get in touch!

@hippodigitaluk

info@hippodigital.co.uk

hippodigital.co.uk

hippodigital