BRIDGING THE IDENTITY GAP:

How Biometric Bound Credentials Resolve Critical Deficiencies in Digital Authentication

May 2025

TrustStamp

As digital identity systems continue to mature, the need for robust, user-centric authentication mechanisms becomes more pressing. A review of prominent UK government and industry documents referenced below reveals a collective step in the right direction, yet critical shortcomings remain unaddressed. In particular, while the guidelines have been effective in establishing the binding between the digital credentials conclusively to the legitimate individual during enrolment, the binding between this legitimate individual and the person accessing the device during the authentication phase is assumed but not systematically verified with a high level of confidence according to the guidance on UK digital identity and attributes trust framework [2] which references GPG 45 [7]. Effectively, the digital credentials generated during enrolment can be misused or abused by anyone who can unlock the device, who is usually someone familiar with the user.

This is the so-called friendly fraud. Biometric bound credentials (BBCreds) [5] present a novel solution that not only addresses these gaps but redefines the standard for secure digital identity.

Although this article is written with references mainly referencing the UK context, the findings are still applicable in general because they are also based on, as well as being consistent with, standards bodies such as ISO, NIST, European guidelines, legislations, and best practices.

Progress in the right direction

The guidelines "Using a Digital Identity to Buy Alcohol Safely and Securely" [1] is correct to address age assurance by addressing three key questions regarding the ID document:

1. **Age check:** Does it show that the person is over 18?
2. **ID-person binding:** Does it belong to the person presenting it?
3. **ID check:** Is it a genuine document?

In a digital world, the ID document must exist in a digital form such as a mobile Driver's license (mDL) or a biometric passport. The latter includes a microchip containing personal information and a digital photograph. In many ways, the above recommendations here are consistent with ISO/IEC 18013-5:2021 [6]. Once all the three checks are successful, an age credential or certificate is issued, which needs to be presented to a relying party every time the age of the credential holder is challenged, during an authentication session.

Currently, a digital credential that is issued after registration is saved on a device. Technically, anyone who can unlock the device can retrieve the credential and act on behalf of the holder. At this point, the identity of the holder is not checked but assumed; in other words, the credential is not bound to the holder. Instead, it is bound to the device where the age check was performed. Therefore, authentication remains an unsolved, and unaddressed issue in verifiable credentials including age check applications, among others. On the other hand, requiring the user to perform the three checks every single time or at a regular interval is high friction and is generally considered unacceptable.

Below, we shall elaborate on the device-centric illusion and then propose a new privacy-preserving biometric scheme which can bind the holder to their credential directly, known as biometric-bound credential (BBCred).

Flawed Assumptions: The Device-Centric Illusion

The UK Digital Identity and Attributes Trust Framework (Gamma 0.4) [2] places the user at the centre of a digital identity interaction model involving identity service providers, holders, and relying parties. However, in practice, the device—not the individual—often becomes the locus of trust. Any party who can unlock the registered device (smartphone, tablet, or laptop) inherits the user's privileges, whether or not they are the legitimate credential owner.

Overly relying on devices can also significantly weaken additional 2FA security measures because the device itself constitutes a single point of failure. Multi-factor authentication is not effective when secondary factors such as SMS or e-mail OTP are accessible on the same device. The same is true for authenticator apps. In the case of a friendly fraud, anyone who knows how to unlock the device would have access to the OTP sent via email or SMS to the same device, therefore, rendering the additional protection ineffective despite them being considered as offering "high protection" according to GPG 44 [3]. Basically, the authentication factors are not independent, making them vulnerable to the attack by just compromising a single device.

Online Remote Credential Check Is Harder Than Physical In-person Check

In "Using a Digital Identity to Buy Alcohol Safely and Securely" [1], the implication that logging into a digital identity app proves ownership of the identity could be misleading in remote authentication. If a child can unlock a parent's device, they can

bypass age-verification systems, rendering the protections meaningless. The article stops short of addressing how to secure the actual user presence during the authentication session, rather than merely checking the credential secured by the device. In contrast, in-person authentication does not suffer from the same problem because the binding between the holder of the credential and its holder can be physically inspected. Consider this: a railcard inspector can visually inspect if someone holds a valid railcard (see https://www.railcard.co.uk) in the following ways:

1. Visually inspect the photo on the railcard to make sure the holder's face matches the photo
2. Ensure that the railcard is genuine.

There is a parallel here between in-person authentication and remote authentication:

- The railcard in the former exists in the form of a digital credential in the latter.
- The visual face inspection in the former must necessarily use automatic facial recognition in the latter. Liveness check must, therefore, be put in place to avoid injection/presentation attacks.
- The authenticity of the credential (i.e., the railcard) can be cryptographically verified. In the former, Railcard has a digital version of railcard which can be read and verified. In the latter, the credential, when signed with the issuing authority's public key, matches the digital signature from the certificate stored alongside the credential.

As a result, many of the guidelines on buying alcohol in-person are harder to realize when doing the same online. There is also the argument that a stronger check is at the point of consumption, and not of purchase. A young person may entrust an older sibling to buy alcohol for them. In the same manner, in the online/digital world where services are consumed, the holder of the credential must be checked at the point of information consumption.

In short, remote authentication is much harder than in-person authentication for several reasons.

1. Remote authentication requires automatic proof of presence, which is more easily subject to injection and presentation attack. Compared to in-person authentication, in the case of face identification, such attacks may amount to facial disguise or heavy make-up which can arguably be more easily detected without software.

2. Biometrics must be handled in a privacy-preserving manner, without compromising the holder's identity. On-device biometric authentication is appealing because the service provider does not need to store or handle the biometric templates. Unfortunately, since multiple ways can be used to bypass biometric unlocking, such as passwords or patterns, this renders on-device biometric authentication unreliable.
3. Few technologies can reliably bind the credential to the holder reliably, at a high confidence [7], at the point of information consumption.

This makes remote authentication the weakest part of the process in digital/verifiable credentials. A robust implementation of BBCreds can address the above three points.

Credentials and Identity: The Unresolved Gap

The NCSC's guide on biometric systems [4] explicitly states that it does not "consider the assignment of identities to individuals via biometrics". By extension, it cannot be used to link a legitimate credential to its holder. This does not, in any way, reduce the usefulness of the guidelines because they are useful to guide practitioners when using a biometric system to compare two biometric templates -- a reference and a probe sample. One reason for the above binding limitation is that the guide has not yet considered privacy-preserving biometrics technologies along those described by ISO/IEC 18013-5:2021 [6]. Specifically, an enhanced version of biometric cryptosystem has the capability of making such binding possible, resulting in a biometric-bound credential.

As we have already established, binding the credential to the legitimate holder is a foundational requirement for trustworthy and effective digital credentials. Otherwise, anyone can claim a digital credential as their own, even if the digital credential is legitimate. This position highlights a systemic gap: biometric traits are used during the issuance of the credential but are not functionally bound to the digital credentials. Consequently, biometric use is reduced to superficial access control rather than secure verification of the credential.

To illustrate the above point, let us consider the transitivity of binding, making a distinction between a device-centric trust chain versus a user-centric trust chain.

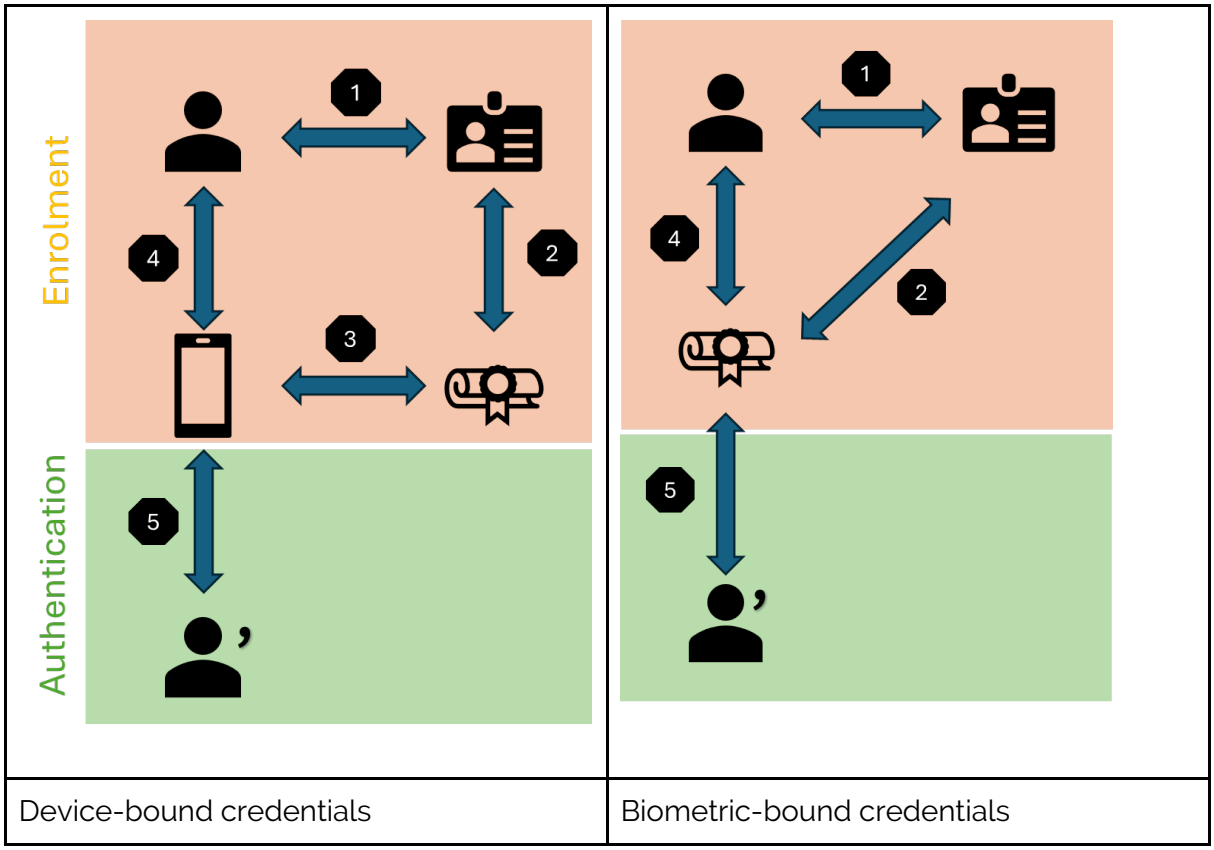


Figure 1: Transitivity of bindings for device-bound credentials versus biometric-bound

In a device-bound credential, several binding types are established:

1. Verify the ID document belongs to its holder, i.e., Alice, the registered user. In this sense, the ID document can be confirmed to be bound to Alice. Note that this binding is bidirectional, i.e., binding A to B is the same as binding B to A.
2. Generate a credential (stored inside a certificate) and bind it with the ID document (which represents Alice's identity).
3. Store the credential on the device. For our purposes, the credential is considered bound to the device.
4. The device is owned by Alice. For our purposes, Alice is bound to the device in order to access the credential. This completes the registration and issuance of the credential.
5. During authentication, Alice' (reads Alice prime) needs to unlock the device in order to access the credential. There is no assurance that Alice' is Alice. Anyone who can unlock the device can act on Alice's behalf.

In contrast, with biometric-bound credential, the following steps are taken.

1. Verify that Alice is the holder of the presented ID document

2. Generate a credential for a specific purpose that is based on Alice's ID document (e.g., this can be the age attestation, university degree certificate, etc).
3. Skip
4. Bind the credential to Alice's biometrics using a registered device.
5. During authentication, the credential is recreated from Alice's device upon her completion of her selfie capture.

The key difference between the device-bound credential and BBCreds is that the credential is bound to Alice's biometrics; and not strictly to the device itself. The device is used as a computer platform to capture and process Alice's biometric sample. Additionally, the device can also serve as an independent second factor (in addition to Alice's biometrics). Therefore, unless a device has been registered or provisioned, it cannot be used for authentication. Similarly, in Alice's absence, it is not possible to generate or "unlock" the certificate, achieved using standard decryption (to be explained further). In short, with biometric bound credentials, a user purported to be Alice (that is Alice') must be the same as Alice (biometrically speaking), and furthermore, as an additional security feature (but not an inherent algorithmic property of biometric cryptosystem), she must also use a device that has been provisioned to prove her remote presence over the Internet. The outcome of this proof is the certificate that is bound uniquely to her.

A New Approach: Biometric Bound Credentials

Biometric bound credentials (BBCreds) offer a powerful remedy by linking a digital credential directly to the legitimate user's biometric characteristics—not to the device. The key properties of this approach include:

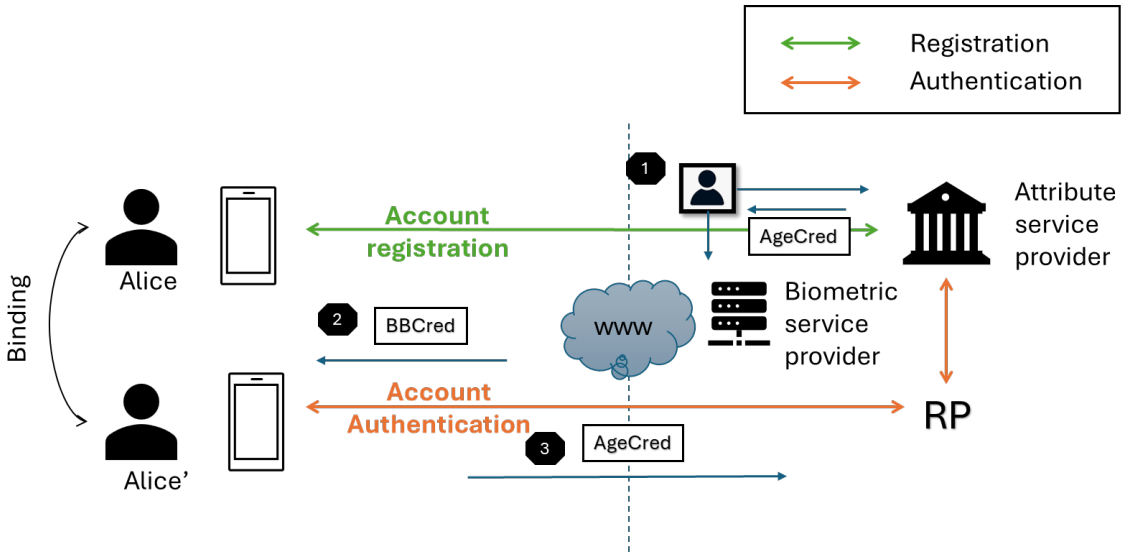
1. **Cryptographic Stability:** Using biometric cryptosystems (e.g., ISO/IEC 24745), a stable cryptographic key is extracted from a live facial image or video during capture.
2. **Decentralization of Secrets:** The resulting biometric bound credential does not store the biometric template or the underlying age credential—ensuring it cannot be exploited even if intercepted.
3. **Liveness and Trust at Authentication Time:** At each login, the same cryptographic key must be regenerated in real-time via a liveness-verified biometric probe. This ensures the user present is the one originally registered.
4. **Zero Knowledge Proof Biometrics:** Thanks to the use of a biometric cryptosystem (ISO/IEC 24745) [6], no parties hold the biometric templates – not even the biometric service provider, or the attribute service provider, or

the device itself. This is because the BBCred does not contain any biometric information.

In a practical age assurance context, for instance, only the legitimate user can unbind the age credential, making it impossible for a child with access to a parent's or an older sibling's phone to bypass authentication. This deters friendly fraud by eliminating device-centric assumptions and enforcing person-centric authentication at the moment it matters most. At the same time, only the registered child can access the age-appropriate content.

Protocol: How it works

Below is a simplified explanation of how a biometric cryptosystem can work towards supporting age verification. By abstracting away secure but important implementation details, the reader can better understand the core value that a biometric cryptosystem offers in binding the registered user to their credential, whilst performing biometric authentication. This is truly a paradigm shift in biometric comparison because biometric templates are not directly used; instead, the comparison is reduced to comparing binary strings.



Step 1: Issuance of AgeCred and BBCred

During account registration, a user, Alice takes a biometric capture, which can be a selfie image or a video. The liveness of the capture is assessed to detect any possibility of injection attack and presentation attack. The same data is passed on to the attribute service provider whose responsibility is to provide an attestation of the age of the individual. Refer to [9] regarding various ways of establishing the age of a person with different degrees of effectiveness, ranging from using open-banking and

mobile network operator checks, to digital identity services and age estimation, among others.

Upon successful checking, an age credential, "AgeCred" is issued and passed back to the biometric service provider. The registration completes by combining the AgeCred with a stable key extract from the biometric capture.

$$BBCred = Encrypt(AgeCred, StableKey)$$

Step 2: Issuance of the BBCred

The biometric bound credential, BBCred, generated is then stored on Alice's device. Anyone who manages to unlock Alice's device cannot unlock the AgeCred which is from just the BBCred. Alice must really be present and subject to the same capture process.

Step 3: Unbinding of the AgeCred

During authentication, Alice will undergo the same biometric capture process of the biometric service provider. This process can happen on a device without needing to access the internet. For example, the biometric service provider provides an SDK that runs on Alice's device.

Provided that the StableKey' extracted from the capture is the same as the original StableKey during decoding, the original valid AgeCred can be recomputed:

$$AgeCred = Decrypt(BBCred,StableKey')$$

The requirement of StableKey=StableKey' means that only Alice can reproduce the valid AgeCred, thus proving to the relying party that she and only she (and no one else) is at the other end of the Internet, right now, with the right device (on which the BBCred was saved).

More details about BBCreds can be found in [5].

Limitations of BBCreds

While BBCreds can resolve the gaps in digital authentication, they have some weaknesses related to the nature of biometrics.

- **False acceptance due to similar-looking visual appearance.** Since automatic face recognition cannot distinguish twins or individuals that look extremely similar, if not identical, then it is impossible to use face biometrics alone to tell them apart. Adding a second biometric modality such as iris, fingerprint or palmprint can address this since these biometric patterns are not dependent on DNA; so, can tell twins apart.
- **False rejection due to adverse capture environments**. Images captured in poor illumination condition may cause the underlying decoding algorithm to fail, therefore, unable to reproduce the StableKey' to match the original. To this end, an active UI capture providing user feedback can guide the user to providing a high-quality selfie photo. E.g., the active guidance can include: "move to a brighter location", "look into the camera" and so on, so that a frontal face image can be captured under good lighting conditions.
- **False rejection due to significant changes in the biometrics**. Significant time gaps between the enrolment sample and a probe sample can cause the decoding to fail. To this end, successful decoded samples can be used to update the enrolment samples, in a solution known as adaptive biometric systems [10] or template updating.

Despite these weaknesses, the progress in biometrics and deep learning has made it possible to attain accuracy operating at a false acceptance rate of one in a million, as attested by NIST's Face Technology (FRTE/FATE) Evaluations, making the solution widely used and accepted by the public, commerce and government agencies alike. Addressing the shortcomings can further improve the robustness, resilience, and usability of the technology.

Reimagining Digital Trust

By shifting the trust anchor from the device towards the user, biometric bound credentials represent a transformational upgrade over existing methods. Unlike the references reviewed—which emphasize frameworks, protocols, and interfaces—BBCs prioritize authentic presence, ensuring that digital systems respond only to the true credential holder.

As governments and service providers look to scale digital identity solutions, adopting biometric bound credentials could bridge the persistent trust gap and pave the way for more secure, privacy-respecting, and fraud-resistant authentication systems.

References

[1] "Using a Digital Identity to Buy Alcohol Safely and Securely." Enabling Digital Identity, 21 Dec. 2024, https://enablingdigitalidentity.blog.gov.uk/2024/12/21/using-a-digital-identity-to-buy-alcohol-safely-and-securely/ , accessed on 2025-04-23

[2] "UK Digital Identity and Attributes Trust Framework: Gamma 0.4 (Pre-Release)." GOV.UK, Government of the United Kingdom, accessed on 2025-04-23, https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-04/uk-digital-identity-and-attributes-trust-framework-gamma-04-pre-release.

[3] "Authentication Credentials for Online Government Services." GOV.UK, Government of the United Kingdom, GPG 44, https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services, accessed on 2025-04-23

[4] "Biometric recognition and authentication systems: Understanding biometric recognition technologies, and how to build secure authentication systems." National Cyber Security Centre, UK Government, https://www.ncsc.gov.uk/collection/biometrics, accessed on 2025-04-23

[5] Biometric-Bound Credentials: A New Era in Digital Identity. Norman Poh, https://blogs.truststamp.ai/revolutionizing-security-with-biometric-bound-credentials-a-new-era-in-digital-identity

[6] ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence, Part 5: Mobile driving licence (mDL) application. https://www.iso.org/standard/69084.html , accessed on 2025-05-02

[7] "Identity Proofing and Verification of an Individual: How to prove and verify someone's identity." GOV.UK, GPG 45, https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity, accessed on 2025-05-03

[8] National Institute of Standards and Technology. "Identity Proofing." Digital Identity Guidelines. National Institute of Standards and Technology, https://pages.nist.gov/800-63-3/sp800-63-3.html , accessed on 2025-05-03

[9] Ofcom, Guidance on highly effective age assurance, https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf , assessed on 2025-05-03

[10] Pisani, P. H., Mhenni, A., Giot, R., Cherrier, E., Poh, N., de Leon Ferreira de Carvalho, A. C. P., Rosenberger, C., & Ben Amara, N. E. (2019). Adaptive biometric systems: Review and perspectives. ACM Computing Surveys, 52 (5), 5, Article No.: 102, Pages 1 - 38.

Contact Information

For technical correspondence, please contact:
Dr. Norman Poh
Chief Science Officer
npoh@truststamp.ai

TrustStamp

TrustStamp