Using UK Trust Framework certified Digital IDs to add evidentiary weight to eSignatures

July 2023 | Version 1.0

Produced by: Nick Mothershaw, on behalf of the OIX / TISA eSignatures working group

Table of Contents

1 BACKGROUND, SCOPE AND PURPOSE

Our working group previously produced the Explaining eSignatures paper, which explores the different of eSignature: Simple, Advance and Qualified and their legal applicability.

A separate paper, the Market Opportunity for eSignatures with a Qualified Certificates, explores how UK Digital identity and Attributes Trust Framework certified Digital IDs can be used as the qualifiers to obtain Qualified Certificates for QES.

The purpose of this paper is to highlight the opportunity to use UK Digital identity and Attributes Trust Framework Certified Digital IDs to add evidentiary weight to a simple or advanced electronic signature through association of a ‘known user’ with the electronic signature. The paper explores how this would work and what use cases this may be applied to.

Please note that this document does not represent the views of Ofcom.

2 INTRODUCTION

Simple electronic signatures are widely used in the UK market today, through a variety of signing platforms such as Adobesign and Docusign.

These dedicated electronic signature software platforms allow a company or an individual to send important documents to anyone in the world using a computer or smartphone through trusted electronic signature software. Once received, the recipient can input their signature, accept the terms, and send it back in less than a minute.

The key feature of these platforms is that they store a cryptographically signed electronic record of the signing event for each party. They form a system of record for these events and the information stored in these events may be used in court as evidence that a party agreed to the documents.

The issuer of the document to be signed typically invites the signee to take part in the electronic signing process by sending them a link to the document on the signing platform by email. The signatory then uses an account they have with the signing platform for their email address to execute the electronic signature. If the user does not have an account for the signing platform they may need to create one using their email address the first time they use the platform.

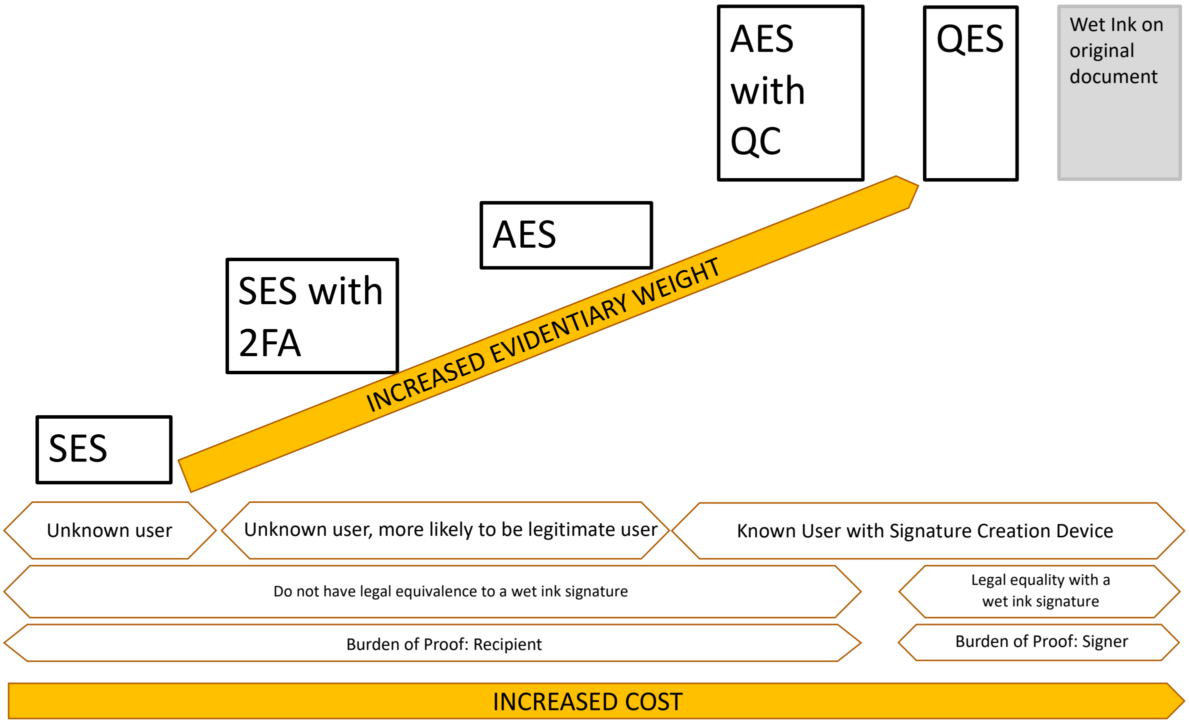
It is also common practice when using electronic signature software platforms to send a PIN to the signatory by telephone call or by text which must be entered to access the document. A PIN provides two-factor authentication to combat the risk of a signatory's email inbox being compromised. This adds to the electronic evidence trail, and may provide additional clarity as to the identity of the signatory if the validity of signature were to be challenged.

However, the user is not verified as being who they claim to be as part of this process. The process confirms that this user in in control the email address and phone number provided, but not that this user is the intended signatory of the document. The evidence of signing held by the platform might be refuted by the user in court as having been created by an imposter. In particular if the email and phone can be shown to have not been owned by the genuine user.

This is where using a UK Trust Framework Certified Digital ID where the user has been verified to a recognised government backed standard will help.

3 EVIDENTIARY WEIGHT

The progression from simple electronic signatures, though advanced electronic signatures to qualified electronic signatures increases the evidentiary weight of the eSignature:


AES with QC
QES
Wet Ink on original document
AES
SES with 2FA
INCREASED EVIDENTIARY WEIGHT
SES
Unknown user
Unknown user, more likely to be legitimate user
Known User with Signature Creation Device
Do not have legal equivalence to a wet ink signature
Legal equality with a wet ink signature
Burden of Proof: Recipient
Burden of Proof: Signer
INCREASED COST

The evidentiary weight increases as the user becomes a “known user”. Today two factor authentication (2FA) is often used to ensure the user signing the document is in control of the login they are using to sign the document. However, this does not mean the user has been proofed to any recognised standard and is therefore “known”, it simply helps verify that this is the same user who set up the account adding some legitimacy.

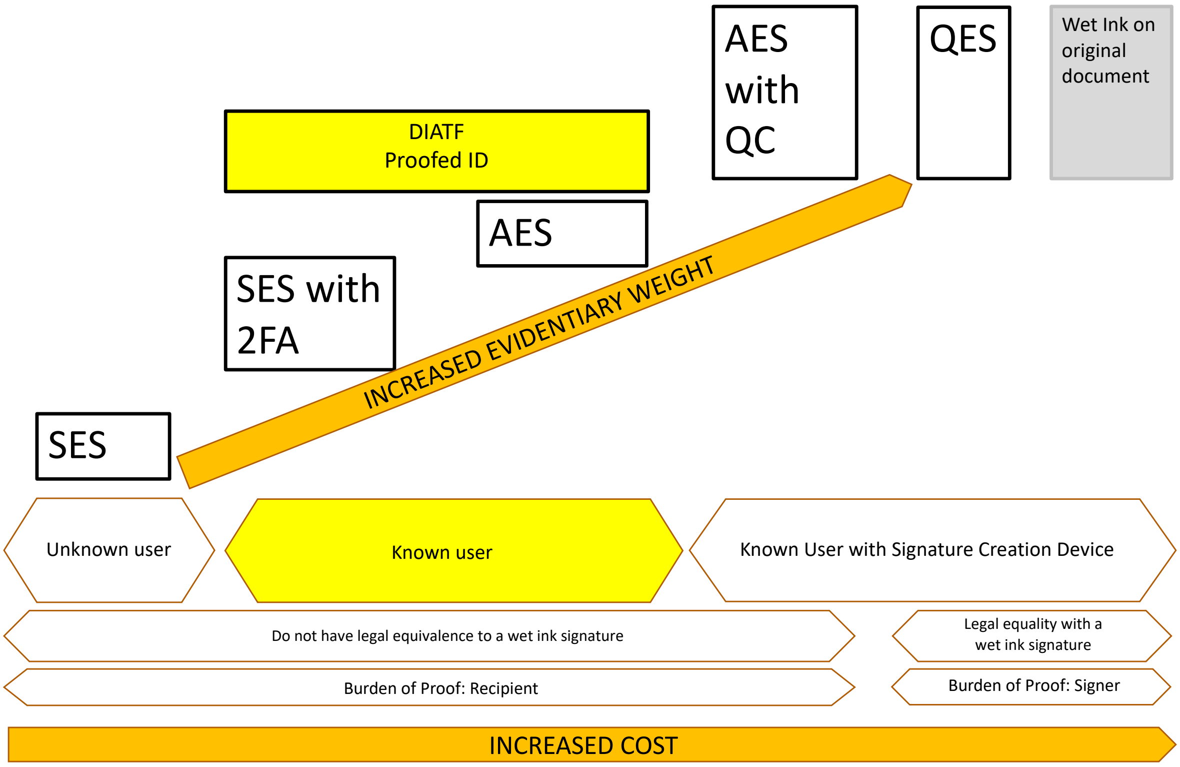
Can Digital ID help to add to evidentiary weight by providing confidence that a “known user” is signing the document, but without going as far as issuing a qualified certificate?

4 USING A TRUST FRAMEWORK CERTIFIED DIGITAL ID TO SIGN

It is now possible for UK citizens to create a (reusable) Digital ID with a UK Digital Identity and Attributes Trust Framework (DIATF) certified private sector Digital ID Provider (IDSP). To obtain a certified Digital ID the user goes through an identity proofing and verification process to a defined standard and thus the user's identity can be trusted by organisations that wish to rely on this information.

The proofing process to obtain a Digital ID typically involves the user proving who they are using a photo ID document, such as a passport or driving licence, or a logon to online banking or answering knowledge-based questions. Different proofing "levels of confidence" are defined; higher levels of confidence could be required for higher value transactions.

The use of a proofed Digital ID would add weight of evidence to the signing process as the signature would be by a traceable "known user" and this adds evidentiary weight to whichever signing method is used; SES with 2FA or AES:


AES with QC
QES
Wet Ink on original document
DIATF Proofed ID
AES
SES with 2FA
INCREASED EVIDENTIARY WEIGHT
SES
Unknown user
Known user
Known User with Signature Creation Device
Do not have legal equivalence to a wet ink signature
Legal equality with a wet ink signature
Burden of Proof: Recipient
Burden of Proof: Signer
INCREASED COST

Note that adding a DIATF proofed ID to an SES with 2FA does not automatically make it an AES as the SES does not contain all of the necessary characteristics of an AES. For example, an SES does not contain advanced cryptographic requirements where the signature must be created in such a way that any subsequent change in the data is detectable.

The use of a proofed Digital ID means that the signing platform is "capable of identifying the signatory", which is a requirement for advance electronic signatures.

The signature does not involve the use of expensive signing equipment associated with a qualified electronic signature, nor does it shift the burden of proof to the signer. However, the evidentiary weight behind the electronic signature is increased as the ID for the "known users" is now proofed to a nationally certified standard. Whether the Digital ID provider will take any liability for issue of an incorrect ID is a commercial matter, the UK DIATF does not offer liability cover.

A Digital ID will cost more than sending emails and codes to self-declared users, so implementor will need to make an assessment on whether the additional cost for the additional weight of evidence is worth it.

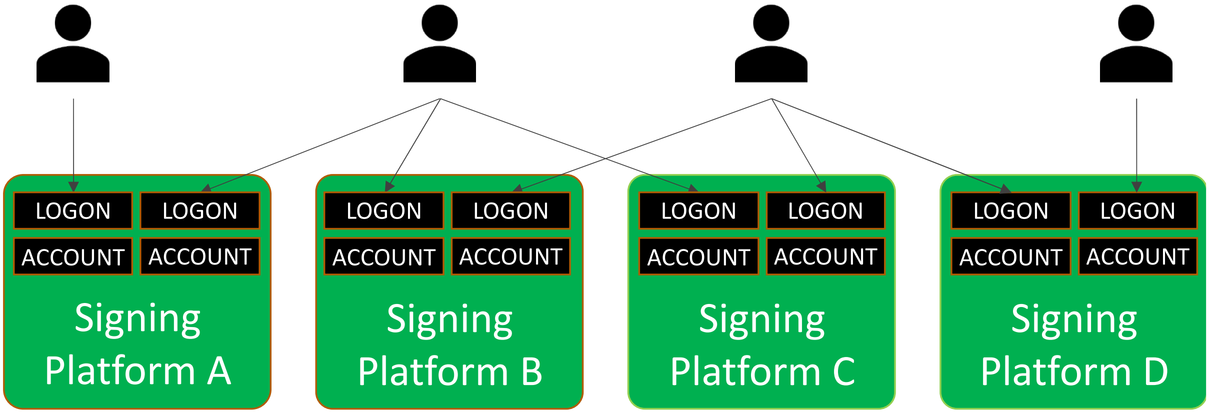
In addition, the use of a Digital ID instead of the use of one-time codes to phones will make for an easier user experience.

Using a Digital ID that the user already possesses will mean the user will merely asserts their Digital ID authenticators to prove it is them, which may be as simple as a phone-based face ID on a known device. This is simpler, quicker and less error prone than sending a one-time code that the user then has to enter back into the system.

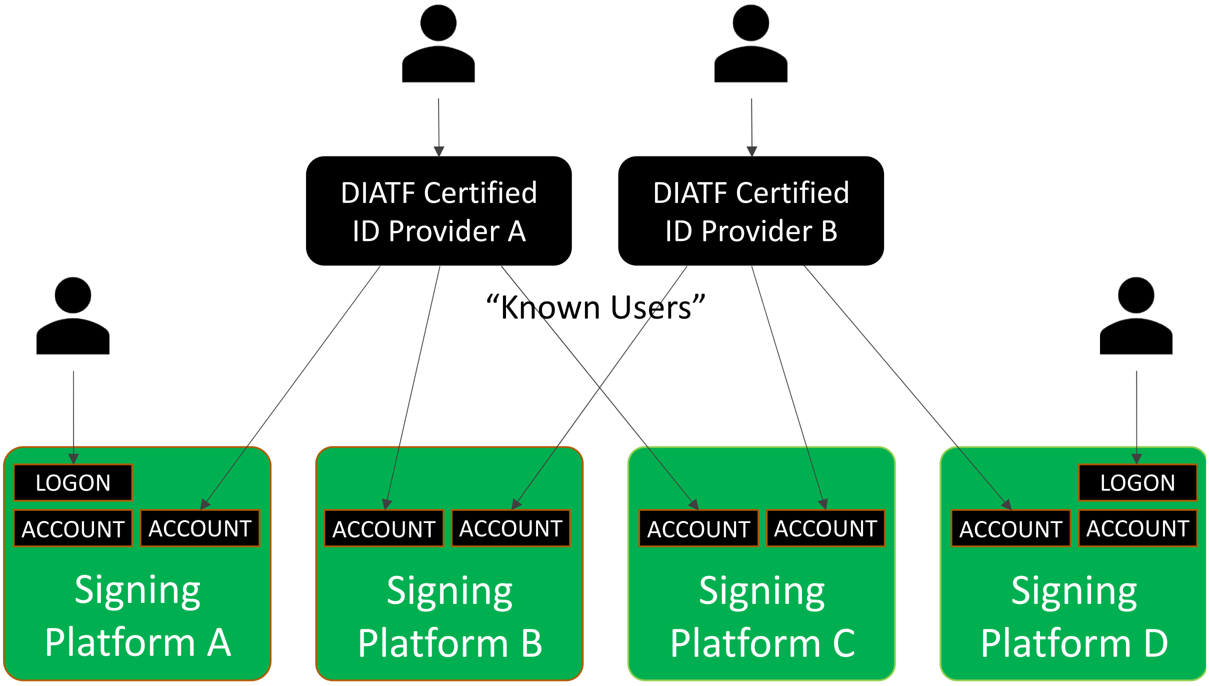
Overall, by leveraging Digital ID for a known user evidentiary weight is increased for less cost than using a qualified certificate and with less user inconvenience.

5 SIGNING PLAFORM USE OF DIGITAL ID

Today, signing platforms issue users with an account for their platform. Users will have a logon and password with many different planforms:



If platforms decide to leverage proofed Digital IDs to improve the evidentiary weight of a Digital signature there is also an opportunity for them to leverage the Digital ID as the way access the platform on an ongoing basis:



On top of the increased evidentiary weight of dealing with a known user, this has several advantages for users and signing platforms:

- Users do not need separate logons and passwords to each platform, they use their Digital ID to prove to the platform who they are. Users therefore do not forget their passwords for the platform and need to do a password reset for each transaction.
- The emails for each user will have already been validated as being in the users control by the Digital ID provider, so no need for email validation.
- Users can instantly sign documents without the need to set up passwords.

6 USE CASES

Our analysis has shown that the following use cases for end consumers are where extra confidence from a DIATF proofed ID would be beneficial.

- Property Rental – could be combined with a Digital ID Right to Rent assertion.
- Employment Contracts – could be combined with a Digital ID DBS check assertion.
- Car Leasing / Hire Purchase
- Financial Services, such as:
    - Automotive Finance
    - Point of Sale Finance
    - Commercial Finance
    - Trust documents in the context of finance
- Life Insurance

7 CONCLUSION

This paper illustrates that there is a clear opportunity to leverage DIATF proofed digital IDs to increase evidentiary weight of simple and advanced electronic signatures.

This opportunity exists in a number of key markets such as: Property Rental, Employment, Car Leasing / Hire Purchase, Financial Services and Insurance.

The opportunity should be explored further. In particular with:

- Signing platforms, such as Adobesign and Docusign.
- DSIT to determine the positioning and promotion of this opportunity within the DIATF.
- Emerging DIATF schemes in the UK as a feature within the scheme portfolio.