Digital Spotlight:

The Role of Qualified Trust Service Providers (QTSPs) in Scottish Retail Banking Practice

Richard Oliphant

Digidentity | docusign

1 / Introduction

In this briefing, I look at the gold standard of electronic signatures – the qualified electronic signature (QES) - and explain its relevance to Scottish retail banking practice.

In Scotland, lawyers favour self-evidencing or probative signatures in banking documents[1], even where this is not strictly required by law. To obtain probative status, a traditional (paper) document[2] is signed in the presence of a witness, and it is presumed to have been validly executed by the signatory.[3]

An electronic document only has probative status under Scots law if it is signed with QES using a digital-signing certificate from a qualified trust service provider (QTSP).

QES is therefore an essential component of every Scottish bank's digital strategy and is the only way to achieve the nirvana of paperless banking. However, the role of QTSPs extends far beyond document execution. They can assist banks (and other financial institutions) in undertaking Anti-Money Laundering (AML) and Know Your Customer (KYC) identity checks on customers.

I also consider the decision by Registers of Scotland (RoS) to accept electronic documents signed with QES in the Register of Deeds in the Books of Council and Session. It signifies that the future of digital conveyancing and land registration in Scotland – and likewise in England & Wales[4] – will be founded on QES.

[1] Particularly in security documents.
[2] A traditional document is one which is written on paper, parchment or some similar tangible surface.
[3] Part 2, section 3 of the Requirements of Writing (Scotland) Act 1995.
[4] https://hmlandregistry.blog.gov.uk/2023/06/15/making-electronic-signatures-and-digital-identity-easier-to-use/

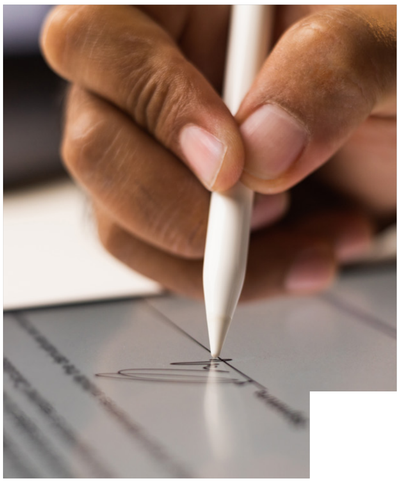
2 / Brexit and electronic signature law

EU eIDAS Regulation (No.910/2014) (EU eIDAS) came into force in July 2016. It established an EU-wide legal framework for electronic signatures and other trust services.[5]

Although the UK left the EU on 31 December 2020[6] (Brexit), EU eIDAS was transposed into UK law by section 3 of the European Union (Withdrawal) Act 2018. The retained law was then modified by a Brexit statutory instrument to create a UK version of EU eIDAS (UK eIDAS).

In this briefing, a reference to eIDAS means both EU eIDAS and UK eIDAS.

3 / Overview of QES



Electronic signatures are ubiquitous. You may be less familiar with QES, but leading platforms such as Docusign offer QES to their customers.

QES is recognised under UK and EU law as the gold standard of electronic signatures.

It is defined in Article 3(12) of UK eIDAS as *"an advanced electronic signature that is created by a qualified electronic signature creation device (QSCD), and which is based on a qualified certificate for electronic signatures."*

QES is a more secure and technologically sophisticated variant of electronic signature. It relies on technology called "public key infrastructure" (PKI). PKI is a protocol under which a trust service provider (TSP)[7] verifies the signatory's identity and issues a qualified certificate (a type of digital certificate) confirming the signatory's name and linking their identity to cryptographic keys known as a public-private key pair (key pair). The more rigorous identity proofing for QES provides greater assurance than other electronic signatures that the signatory is who they claim to be, and that the signed document is authentic. The use of the key pair also prevents any tampering with the document after signing and offers the highest level of document integrity.

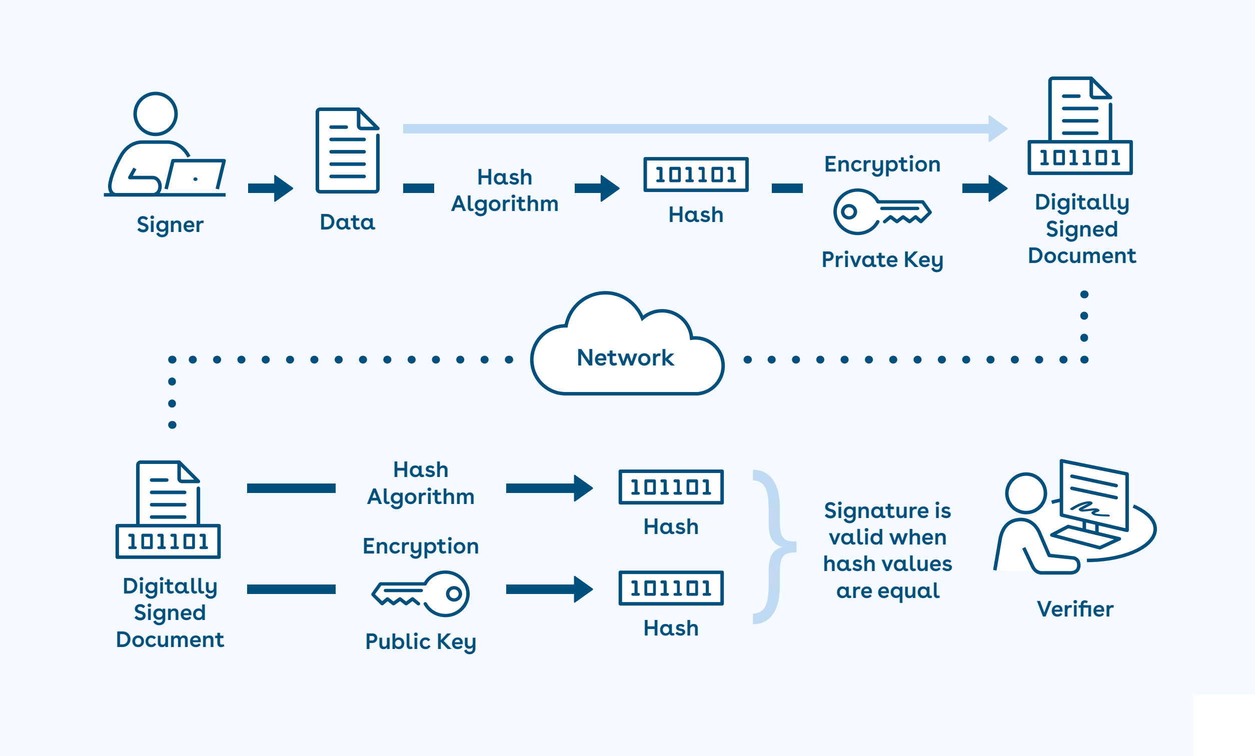
[5] Trust services are defined in Article 3(16) of EU eIDAS. In addition to electronic signatures, trust services include the creation and validation of electronic seals, electronic time stamps, electronic registered delivery services and certificates related to those services.

[6] The UK, in fact, left the EU on 31 January 2020, but the UK and EU agreed a "transition period" which ended at 11pm on 31 December 2020. During the transition period, the UK continued to be treated as if it were still an EU Member State and most EU law, including EU eIDAS, continued to apply to the UK.

[7] TSPs are also known as "certificate authorities" or "CAs". Only a QTSP may issue a qualified certificate for QES.

Creation and validation of QES

The diagram[8] below illustrates how a signatory uses a hash algorithm together with their private key to create the QES. The recipient of the signed document then uses the signatory's public key to decrypt the QES and ensure that the document has not been modified after signature. The recipient also checks that the public key belongs to the signatory and that their qualified certificate was valid at the time of signature *(Article 32, eIDAS)*. PDF documents that are signed with QES on Docusign can be validated using a PDF reader[9] or the European Commission's validation tool.



As well as offering more robust identity verification and cryptographic security, QES has a legal standing which elevates it above the standard Docusign electronic signature, even when that signature is combined with 2-factor authentication[10] *(Article 25, eIDAS)*:

- QES has the equivalent legal effect of a handwritten signature.
- QES based on a qualified certificate issued in one EU Member State shall be recognised as a QES in every other EU Member State and in the UK.[11]

[8] Reproduced from the Interim Report on the Electronic Execution of Documents by the MoJ's Industry Working Group published on 1 February 2022.

[9] For example, Adobe Acrobat Reader.

[10] Typically, an e-signing platform sends a one-time password (OTP) to the signatory as a second authentication factor.

[11] By contrast, one consequence of Brexit is that a qualified certificate for QES provided by a QTSP established in the UK is no longer recognised in the EU. This has created an asymmetry between the UK and EU which has resulted in the UK market being wholly dependent on qualified trust services from EU QTSPs.

4 / The role of QTSPs and remote identity proofing

E-signing platforms may be a QTSP in their own right (such as Docusign)[12] or accept qualified certificates from third-party QTSPs through API integrations. Docusign works with a wide array of QTSPs - notably Digidentity - who issue qualified certificates for signing documents on the platform with QES.

eIDAS subjects QTSPs to a comprehensive regulatory and audit regime which requires them to observe strict security standards. This includes submitting a conformity assessment report to a supervisory body in an EU Member State (or to ICO in the UK), and demonstrating that the QTSP and their QSCD[13] comply with requirements set out in eIDAS *(Articles 20, 24 and 30, eIDAS)*. The regulatory regime is more onerous for QTSPs than for TSPs who provide electronic signatures. This enhances trust in QES and the qualified certificates that underpin the signing process.

Each EU Member State and the UK publishes and maintains its own national trusted list of QTSPs and the qualified trust services they provide *(Article 22, eIDAS)*. National trusted lists have constitutive effect. This means that the electronic signature is *only* a QES if the qualified certificate was issued by a QTSP that appears in a trusted list. The European Commission operates a Trusted List Browser[14] which enables parties to an electronic document to verify that a QTSP is registered in a national trusted list in an EU Member State. The UK trusted list is administered separately by tScheme.

Before a QTSP can issue the qualified certificate, it must verify the signatory's identity in accordance with Article 24 of eIDAS. This traditionally required the signatory to attend a face-to-face meeting, which was slow, inconvenient and expensive. However, the emergence of remote identity proofing now enables QTSPs to offer video authentication of the signatory or – in the case of Digidentity – rapid automated identity proofing with state-of-the-art NFC chip technology.[15]

ETSI has published a new technical standard for identity proofing. It provides some much-needed clarity for QTSPs verifying identity under Article 24 of eIDAS (whether in the EU or UK) and provisioning signatories with a qualified certificate for QES.

[12] For example, Docusign France and Namirial S.p.A. have both been granted qualified status as QTSPs by the national supervisory bodies in France and Italy respectively.

[13] The QSCD will be a hardware security module for remote/cloud-signing, or a USB token or smartcard for local-signing using Adobe Acrobat software. The QSCD must be certified as meeting the requirements in Annex II of eIDAS (Article 30) by a conformity assessment body.

[14] The European Commission publishes an XML document called the "List of Trusted Lists" which consists of links to each Member State trusted list, together with the certificates used to sign those lists.

[15] The user downloads the QTSP's mobile app and uploads a copy of their passport. The QTSP's mobile app uses NFC technology to read the chip in the passport and extract the user's photo. The user then uploads a (video) selfie. The mobile app deploys AI algorithms to match the selfie with the passport photo and validate the user's identity. Once complete, the QTSP issues the qualified certificate to the user.

5 / The transition from local to remote signing with QES

Before the emergence of secure cloud technology, the signatory would create their QES with a private key and a qualified certificate stored locally on a smartcard or USB token. These devices were PIN-protected and plugged into a desktop computer.

However, the combination of the cloud and PKI technology has made it possible for the signatory to sign documents with QES via a web browser or mobile application. This is known as remote signing. The key pair and the signatory's qualified certificate are now hosted remotely by QTSPs on a hardware security module (HSM). The HSM is the qualified electronic signature creation device (QSCD) referenced in Article 3(12) of eIDAS. It must be certified by an approved body as meeting the security requirements set out in Annex II of eIDAS *(Article 30, eIDAS)*.

Docusign has an ever-expanding ecosystem of cloud-based QTSPs whose qualified certificates are compatible with the platform. They have joined with other industry leaders in the Cloud Signature Consortium (CSC) to pioneer an open standard for cloud-based digital signatures[16] that will accelerate the shift away from local signing to remote signing with QES.

As an alternative to the CSC API, Docusign uses its own proprietary API to interface with QTSPs and enable remote signing with QES.

[16] This is an API technical specification for remote (cloud-based) electronic signatures. It defines common protocols for cloud-based QTSPs to securely interface with e-signing platforms. The specification has been adopted as ETSI technical specification 119 432 for remote signature creation.

6 / Electronic documents are permitted under Scots law

Part 10 of the Land Registration etc (Scotland) Act 2012 amended the Requirements of Writing (Scotland) Act 1995 (ROWSA) to allow any document that is required to be in writing under Scots law to be created in electronic form. This excludes wills and other testamentary writings which must be created and signed in traditional form using wet ink signatures.

Until recently, electronic documents were generally not accepted for registration in the Land Register of Scotland, the Register of Sasines or the Books of Council and Session.[17] However, RoS has now signalled its intent to modernise its digital registration service commencing with the decision to open up the Register of Deeds in the Books of Council and Session from 1 October 2022 (see section 9 below).

7 / Electronic signatures and ROWSA

Section 1(2) of ROWSA identifies documents that must be made in writing. They include:

- contracts relating to land (such as missives, dispositions and leases).
- gratuitous unilateral obligations, except those undertaken in the course of business.
- "truster as trustee" trusts.[18]

Section 1(2) documents must be signed with an advanced electronic signature[19] to be valid[20], and QES to be probative.[21]

A probative electronic document is presumed to be validly executed (or authenticated[22]) by the signatory based on its appearance. In a contractual dispute – for example, between a bank and its customer – no further evidence is required from the party founding on the electronic document to prove valid authentication.

Unless there is a specific statutory requirement for a wet ink signature *(e.g. section 31(6) of the Patents Act 1977)*, for documents that fall outside section 1(2) of ROWSA, an electronic signature will be a valid form of execution.

You can find out more about electronic signature law in Scotland by clicking here.

[17] The exception is where QES deeds are registered via the Digital Discharge Service which is wholly controlled by RoS.
[18] Where a person declares himself to be sole trustee of his own property (or any property which he may acquire).
[19] The criteria for an advanced electronic signature (AES) are set out in Article 26 of eIDAS. Like QES, AES relies on PKI technology and a digital certificate to identity the signatory. But QES has more onerous requirements for digital certificates (Annex I of eIDAS) and for signature creation devices (Annex II of eIDAS).
[20] Regulation 2 of the Electronic Documents (Scotland) Regulations 2014.
[21] Regulation 3 of the Electronic Documents (Scotland) Regulations 2014.
[22] For electronic documents the presumption of validity is more accurately termed the presumption of *"authentication"* (Part 3, section 9C of ROWSA).

8 / QES in Scottish banking transactions

Banks may favour the use of QES because (i) it is mandatory under Scots law or (ii) if not mandatory, they prefer the electronic document to have probative status.[23]

There is, however, another compelling reason why banks should consider QES when onboarding retail customers. The modern breed of QTSPs can do *more* than facilitate electronic execution of documents. QTSPs have a toolset for remote electronic identification and verification of customers to satisfy the bank's own AML[24] and KYC requirements at the same time as they issue the qualified certificate. Alternatively, the QTSP may rely on the AML/KYC ID checks undertaken by the bank to issue the customer with a qualified certificate.[25] What matters is that banks work with QTSPs to create a process in which the customer is asked to verify their identity just once.

The capabilities of QTSPs are both under-utilised and misunderstood in UK banking. This is set to change. The European Banking Authority (EBA) has published new guidance which promotes the role of QTSPs in facilitating remote customer onboarding of customers in financial services. The guidance has been adopted by EU financial supervisory bodies. It illustrates, among other things, how QTSPs can help banks and other regulated entities discharge their responsibilities under the EU AML regime. This regime mirrors the UK AML regime and it is to be hoped that the Financial Conduct Authority will also adopt the EBA's guidance in due course.

9 / QES in real estate transactions

RoS opened up the Register of Deeds in the Books of Session and Council on 1 October 2022 for signing deeds digitally with QES. It is also possible to submit "mixed format" deeds (a mix of wet ink and QES) for registration. Any electronic document or deed submitted to RoS must satisfy the existing requirement for probative signatures in Part 3, section 9G of ROWSA.

At the time of writing, RoS has yet to confirm when it will open up the Register of Sasines and the Land Register of Scotland for digital execution with QES. However, this is likely to follow in due course as confidence in, and familiarity with, QES grows.

[23] Section 7.3 of the Law Society of Scotland's guide to electronic signatures advises that *"In certain sectors, the usual practice by solicitors is to seek to obtain a self-proving signature even if that is not legally required. Whether this is necessary should be considered on a case-by-case basis."*
[24] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019; requirements found in the SYSC within the Financial Conduct Authority Handbook; and the JMLSG Guidance.
[25] Article 24 of eIDAS is flexible and allows for the possibility of the QTSP relying on a third party to verify an individual's identity *"in accordance with national law"*.

10 / Why choose Digidentity?

Digidentity is pre-eminent among the QTSPs in the EU Trusted List.

They are unique in being the only QTSP that has been certified as an identity provider against the rules and standards of the new UK Digital Identity & Attributes Trust Framework.

They have an API integration with Docusign. This enables Docusign to offer Scottish customers the ability to outsource electronic identification and verification to Digidentity as part of their AML and KYC identity checks, and to create probative signatures under Scots law.

Richard Oliphant is a consultant to Docusign, Adobe, Digidentity, CMS, HM Land Registry, OneID and the Cloud Signature Consortium. He specialises in electronic and digital signature law and practice, and in digital identity schemes. He is also the author of the Practical Law practice note on e-signing platforms and electronic signatures.

This paper is made available for general purposes and guidance only and does not purport to constitute legal or professional advice.