Market Opportunity for eSignatures with a Qualified Certificate based on Digital Identities

February 2023
Version 0.10

Author: Nick Mothershaw
on behalf of the OIX eSignatures working group

1 TABLE OF CONTENTS

2 BACKGROUND AND SCOPE

2.1 Different Types of eSignature

The TISA/OIX eSignatures working group previously produced the Explaining eSignatures paper, which explores the different types of eSignature: Simple, Advanced and Qualified and their legal applicability. This paper assumes readers are familiar with the different types of eSignatures.

2.2 UK Market - Where we are today

The market for the 'gold standard' of Qualified Electronic Signatures (QES) in the UK is relatively immature in comparison to our European neighbours. There are several reasons for this, which include:

1. Lack of knowledge and understanding of the benefits;
2. Low comprehension of the process and legal effect and evidentiary weight of QES;
3. Absence of case law highlighting the risks of using lower levels of electronic signing;
4. Integrating a new process that is on the surface more expensive;
5. Apathy relating to the adoption of a new process and the transition from analogue to digital;
6. High Cost of QES – a qualified certificate for QES can exceed £100 per annum;
7. It is not possible to get a qualified certificate issued in the UK, that can be used in the EU. UK based users must get a qualified certificate from a qualified trust service provider (QTSP) listed in the EU trust list to issue qualified certificates which are recognised across the 27 EU member states.

As a result, in the UK, QES is only occasionally used for high value or cross border business-to-business transactions.

The situation in Scotland is slightly different; The QES market is further ahead in Scotland due to the introduction of QES by the Registers of Scotland and requirements for 'probative' or 'self-proving' signatures which can only be fulfilled with QES.

The recent restrictions on our physical interactions due to Covid-19 proved there is an even greater, and more obvious, need for a remote way to prove who we are with a high degree of confidence and sign legal agreements.

2.3 UK Market – Post Brexit

Post Brexit, the UK is able to accept qualified certificates for QES from QTSPs registered in EU member states. However, the EU Commission has not extended that mutual trust to UK QTSPs. This means that there is potentially a supply issue for the UK market in terms of where individuals and organisations go to source qualified certificates for QES. This poses

some potential challenges. QES is a natural extension of an identity verification process. The UK recognises the importance of a digital economy founded on a robust and mature Identity ecosystem and is progressing the next stage of that ecosystem through the UK Digital Identity and Attributes Trust Framework. In every case, a user's digital identity is the foundation for a QES. Therefore, from a user's point-of-view, having an identity, which can't be converted into a QES for use outside of UK borders undermines its value.

2.4 Scope

This paper explores the UK market opportunity for remote signing using eSignatures that are supported by a qualified certificate. That could be either:

- An Advanced Electronic Signature with a qualified certificate; or
- A Qualified Electronic Signature.

3 BENEFITS OF ESIGNATURE WITH A QUALIFIED CERTIFICATE

Although there is a certain amount of ambiguity surrounding what level of eSignature is required for specific use cases governed by UK law, there are undoubtedly benefits in being able to securely sign documents remotely.

General benefits of using simple e Signatures include:

- Removing the need for the individual to attend a physical location to sign a document
- Significant reduction in the time taken to complete the signing process particularly where multiple signatures (and witness attestations) are required
- More cost effective in terms of hard copy production & postage
- Some eSignature providers will take liability for the validity of the signature subject to a contractually agreed financial cap.

The additional benefits of using a Qualified Certificate include:

- It is legally equivalent to a wet-ink signature on an electronic document.
- More secure process in terms of the assurance of the identity and integrity of the document. The signature is bound directly to the document by encryption. This ensures a higher level of document integrity (i.e., cannot tamper with or modify the document post-signing).
- Document storage is likely to be electronic, allowing the signed document to be easily retrieved when required. Whereas signed paper documents can be very difficult to find.
- Legal burden of proof moves to the signer.

As a further example, UK Land Registry introduced the ability for individuals to “sign” their re-mortgage deeds online using their GOV.UK Verify digital identity, which in future will move to leverage a UK One Login for Government ID. This is not an electronic signature though, but a use of a Digital ID in lieu of a wet ink signature for the purpose of adding a charge to the land registry entry. See https://www.gov.uk/government/news/hm-land-registry-is-making-it-easier-to-remortgage

The following paragraph is an extract from the Land Registry article: *The digital service enables people to sign their mortgage whenever and wherever they are, including on their phone or computer. It removes the need for ‘wet’ (pen-on-paper) signatures, and witnesses no longer need to be present when the documents are signed. Homeowners no longer face delays from having to print out forms, find an independent third party to witness their signature, and pay to return the forms by post.*

4 UK QTSPS AND THE UK TRUST FRAMEWORK

It is possible to use a UK Digital Identity and Attributes Trust Framework (DIATF) certified Digital ID as the verification method in order to issue a user a qualified certificate.

The following text is from the UK Information Commissioners guide to eIDAS, specifically the section on Qualified Trust Service Provider Obligations:

How should we verify the identity of our customers?
If you are a qualified trust service provider, UK eIDAS Regulation Article 24(1) requires you to verify the identity of any individual or organisation to whom you issue a qualified certificate. It sets out four verification options:

- *in person, by the physical presence of the person or authorised representative of the organisation;*
- *using electronic ID that was itself originally verified in person, and meets the eIDAS assurance level of "substantial" or "high" set out in EU eIDAS Regulation Article 8;*
- *using a certificate of a qualified electronic signature or seal that was itself verified in person or using electronic ID as set out above; or*
- *using another method recognised by the UK government which is confirmed by a conformity assessment body as being as reliable as verification in person. If you choose this option you will need to provide evidence that this is the case.*

It has been confirmed to OIX by DCMS that the DIATF is "another method recognised by the UK Government".

The ICO guidance goes on to say: "You can carry the verification out yourself or use a subcontractor", which means QTSPs are free to use a third party DIATF certified IDSP (Identity Service Provider) to undertake verification for them. The user can then be issued a qualified certificate from the QTSP.

However, it is not clear from the current ICO guidance what level of confidence for proofing, and what type of authenticators the DIATF certified digital ID should have to be accepted as the verification method to issue a qualified certificate.

As the level of assurance for the EU is set at "substantial" or "high", OIX proposes that the UK levels for accepting a user when issuing at qualified certificate should be:

- GPG45 Level of Confidence of "medium" or higher,
- GPG44 Authenticators of "high protection".

OIX has proposes that there are 2 routes to address this:

a) DCMS directs that the ICO guidance be updated to contain a bullet point with the following wording:

    - *using digital verification services under the DVS Trust Framework that meet a Level of Confidence of "medium" / "high" / "very high", with authenticators of "high protection".*

b) *DCMS updates the UK Digital Identity and Attributes Trust Framework to state:*

- *ICO Guidance states that Qualified Trust Service Providers may use a digital verification service that is a "method recognised by the UK government which is confirmed by a conformity assessment body as being as reliable as verification in person". This Trust Framework is such a method recognised by the UK government. When verifying the user via this trust framework the users ID should meet a Level of Confidence of "medium" / "high" / "very high", with authenticators of "high protection".*

Once the user has been verified using a DIATF Digital ID, the QTSP could then allow the IDSPs' Digital ID to manage access to their platform to assert the QC as part of a QES.

5 OPTIONS FOR QTSP AND IDSP COLLABORATION

OIX analysis has identified several different ways IDSPs and QTSP can collaborate, which are summarised in the table below. The table only covers the options for remote signing through a QTSP service:

Scenario	Who Verifies the User?	Who Issues and manages (revokes) the QC?	Who stores the QC?	Who manages the QC private key?	How does the user assert the QC?	How does the user access the QTSP service?
Scenario 1	A DIATF certified IDSP	The QTSP Certificate Authority	The QTSP	The QTSP	Via QTSP issued Authenticators (issued to GPG44 standard).	Via QTSP issued Authenticators (issued to GPG44 standard).
Scenario 2	A DIATF certified IDSP	The QTSP CA	The DIATF certified IDSP	The QTSP	Via DIATF certified IDSP Authenticators	Via QTSP issued Authenticators (issued to GPG44 standard).
Scenario 3	A DIATF certified IDSP	The QTSP CA	The DIATF certified IDSP	The QTSP	Via DIATF certified IDSP Authenticators	Via DIATF certified IDSP Authenticators
Scenario 4 -	The QTSP for GPG45 standard	The QTSP CA	The QTSP	The QTSP	Via QTSP issued Authenticators (issued to GPG44 standard).	Via QTSP issued Authenticators (issued to GPG44 standard).

Note that in all scenarios the QTSP must issue the qualified certificate (QC) and must manage the QC key in a Qualified Signature Creation Device HSM.

In Scenario 4 the QTSP will also most likely be a DIATF certified IDSP in its own right.

6 MARKET APPETTITE

Is there a broader appetite for the use of e-Signatures with a Qualified Certificate that allow remote signing? We believe there is as:

- People want to do more online
- COVID-19 drove the expectation for non-face-to-face methods of engagement
- Lower cost of doing business
- Increase speed of transactions
- Competitive position
- Drivers:
    - Remote interactions
    - Ease of use
    - Confidentiality
    - Security (harder to forge than wet ink)
    - Greater evidentiary weight in court proceedings
    - Environmental – more sustainable - reduced paper
    - Speed of completion (especially international transactions)
- Using a QES could take away the need for a document to be witnessed, saving time.

Leveraging a UK DIATF certified Digital ID to proof a user for a Qualified Certificate and then to subsequently access the e-signing platform to sign documents is a significant enabler for several of the drivers outlined above, including: doing more online, ease of use, lower cost and increased speed.

Whilst there is appetite in the market, there is also a big educational gap to spur adoption. There is a need to de-mystify how this works. This paper aims to aid this demystification.

7 LOWERING COSTS

In order to satisfy this appetite, lower costs for qualified certificate are required.

Leveraging DIATF certified IDSP for verification and authenticator management is one-way costs will be lowered. DIATF certified IDSP will offer modern re-usable two-factor authenticators that can be leveraged with the Digital ID across many use cases, thus creating an economy of scale.

Another way costs are reduced is through the cloud-based signing associated with remote signing infrastructures. With cloud-based software, QTSPs use HSMs (Hardware Security Modules) to hold keys on behalf of their users, as opposed to storing the keys on physical hard-ware tokens. A signatory who uses a QTSP offering this service, uses the HSM to securely hold the signing keys, so there is a much lower risk of them being lost or stolen. Signatories can securely sign documents using their smart phone, tablet or another electronic device, which they are much less likely to lose or forget and means that the physical tokens aren't required to be re-issued making for a better experience for all involved and a more sustainable model.

A cloud-based solution can be set up in half an hour. With physical signing devices you could be waiting days, or even weeks, for your signing device to arrive.

eIDAS makes it explicit that cloud-based signing is permissible, thus setting the direction in favour of using cloud-based.

8 USE CASES FOR QUALIFIED CERTIFICATES

There are two sides to the Electronic Signatures with Qualified Certificates market:

1. **The company representative**, e.g., a conveyancer or company director, who uses it many times a week and signs, potentially, hundreds of documents every year; This Employee may be using a personal electronic signature on behalf of the company.
2. **The individual**, who needs it more occasionally to sign significant documents such as mortgage deeds, employment contracts or other legal documents.

Our analysis has shown that the following use cases are where there is a regulatory requirement to use QES and will therefore benefit immediately from remote signing using an eSignature with a QC:

Individual:

- EU Cross Border Trade
    - Commercial Contracts
    - Employment Contracts

Company Representative:

- EU Cross Border Trade
    - Commercial Contracts
    - Employment Contracts

In addition, in Scotland conveyancers can use a signature with a Qualified Certificate to sign documents in relation to property transactions on behalf of their client.

The following use cases are where there is strong argument to use QES and should therefore benefit in due course from remote signing using an eSignature with a QC:

Individual:

- Mortgage Deeds
- Residential Property Conveyancing
- Wills / Probate
- Lasting Power of Attorney
- Employment Contracts (for certain EU countries)

Company Representative:

- Commercial Mortgage Deeds
- Commercial Property Conveyancing
- Commercial Property Rental

A consideration is whether both parties can use QES to sign the document; if both parties cannot use QES then one party may use wet ink signature and the other may use a QES. This leads to complexity in determining the signing trail of the document and also complexity in

court, who seem to favour the party with the electronic signature. Access to lower cost QES capabilities will make it easier for end users to access QES capabilities, making more likely that both parties will have access to QES signing.

It is also anticipated that highly regulated, risk averse sectors such as finance will start to use QES to mitigate risk even where it not a regulatory requirement for their use. This will include signing deeds as well as contracts, in particular involving transactions of a cross border nature.