Discussion Paper: Using QWACS for PSD2 Mutual Authentication

Nick Pope – Thales

14 August 2017

# Introduction

At the ETSI PSD2 workshop on 21st July it was suggested that for PSD2 mutual authentication is required between the TPP (third party payment provider) and the AS-PSP (account servicing payment service provider e.g. bank) on the TLS (transport layer security) connection (see document ESI(17)000110). The connection may go from TPP to AS-PSP or as a ‘call back’ from AS-PSP to TPP .

At this meeting it was suggested that eIDAS Qualified Web Site Authentication Certificates (QWACs or terms of eIDAS ‘qualified certificates for website authentication’) could not be used for TLS client authentication (i.e. for authentication of the calling party). However, it was subsequently pointed out that there is technically no reason why the same certificate cannot be used for TSL client and server authentication particularly in the case where a website is also acting as a TSL client for another website, as is the case of PSD2 TPP / AS-PSP mutual authentication requirement (see email from: Luigi Rizzo 28/07/2017).

This paper considers the eIDAS legal requirements; however it is not aimed at giving a legal opinion. Rather it is aimed at a discussion considering the technical implications of eIDAS, in order to decide whether there is any reason why ETSI should raise possible concerns over the use of QWACs for mutual authentication for PSD2.

This paper does not currently represent any consensus viewpoint in ETSI, although it is aimed at building consensus.

# eIDAS (Regulation 910/2014) Requirements

The concept of website authentication is introduced in recital (67) which states:

*“Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. ……”*

The following definitions are given in Article 3.

*(38) ‘certificate for website authentication’ means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;*

*(39) ‘qualified certificate for website authentication’ means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;*

Article 45 states the following requirements for ‘qualified certificate for website authentication’:

*1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.*

*2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).*

Annex IV states specific requirements on the contents of the certificate.

# Discussion

In considering the above eIDAS requirements the following observations are made:

1. There is no indication in the regulation that the use of QWACs is limited to authentication of the calling (TLS client) or called (TLS server) party. The Article 3 definitions make no reference to any particular use.
2. The recital 67 description of a “visitor to a web site” does indicate an example client / server use case which motivated the support for web site certificates, but this does not state any restrictions on the use of web site certificates. In particular, the “visitor” could also be a website, which itself may have a website certificate. Furthermore, later text in recital 67 makes clear that the regulation aims to give maximise flexibility and follow the lead of the CA/Browser Forum.
3. The requirements given in article 45 and Annex IV give no indication of any restriction of the use of the certificate except that it is used for “website” authentication.
4. Since PSD2 is expected to involve “call back” from the AS-PSP to the TPP the relationship should perhaps be considered as peer-to-peer rather than client-server. So the AS-PSP / TPP cannot be considered as having a fixed client / server role. Technically, there is no reason for the use of a certificate to be fixed to use in a particular role given it is the same entity. As indicated by CAB/Forum document a website certificate may be assigned both roles.
5. Regarding whether a TPP or AS-PSP may be considered as web sites, since both of these entities are providing services over the internet it is not seen how this can be disputed.
6. There is a possibility that customer to TPP or AS-PSP website and interactions between TPP and AS-PSP websites may be via different access points using different domain names. However, there is no indication that this is restricted. Indeed Annex IV(e) indicates that the web site may be access via different domain names, in the single or potentially separate certificates.

With the above technical consideration, there appears to be nothing in the regulation that clearly prohibits the use of QWACs for mutual TSL authentication.