Quali-Sign Ltd

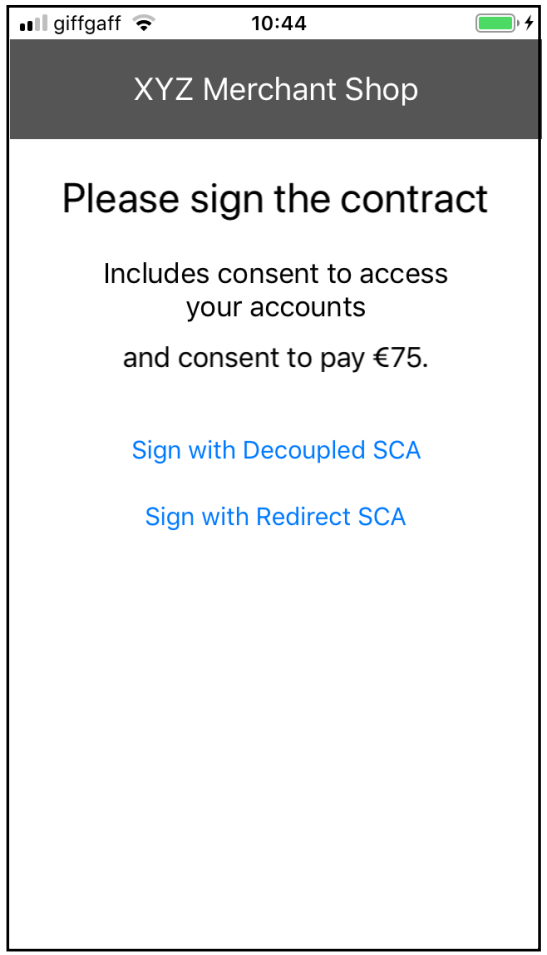
A PSU signs a contract with a TPP using the SCA procedure of their ASPSP

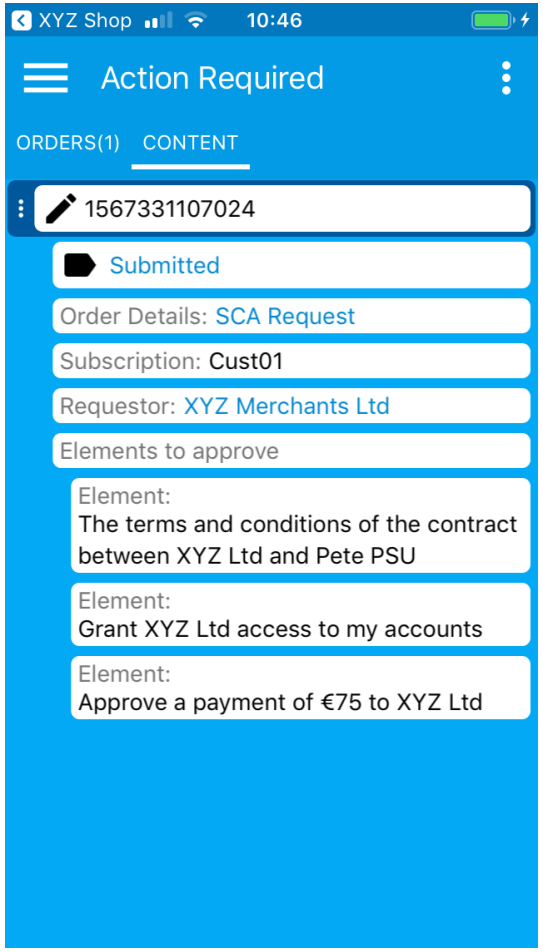
Michael Adams

Tel: +44 7808 203856

1st September 2019

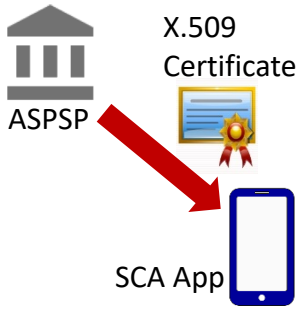
The PSU sign's a TPP contract using their ASPSP's SCA APP. The contract includes consent for the TPP to access the PSU's accounts. It also includes consent to make a payment. This means the PSU only needs to perform SCA once!





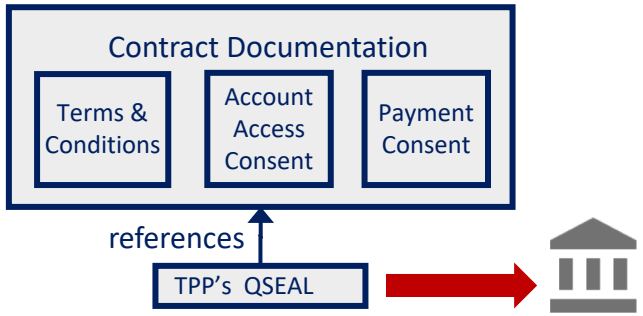
Summary of the Customer Journey

SCA App Enrollment



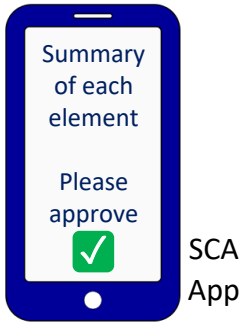
- A PSU installs an ASPSP's dedicated SCA app on their smartphone.
- Once activated, the ASPSP issues the PSU with an X.509 certificate to represent their SCA credentials.
- The app can now perform SCA.

TPP prepares an SCA Request with multiple elements



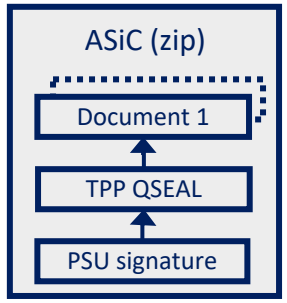
- The PSU visits a TPP web site to perform a single transaction. They have no need for an ongoing relationship with the TPP.
- The PSU is required to make a payment (or series of) to the TPP. The PSU requests the SCT payment method and specifies their ASPSP and related PSU-ID.
- The PSU agrees to the TPP requesting a list of their accounts from the ASPSP, in order to select an account to debit.
- The TPP prepares a contract for the PSU to sign. This includes the PSU's consent for the TPP to access their account(s) and their consent to initiate the payment(s) for a specified amount to the TPP.
- The TPP signs the contract with their QSEAL credentials. The result is a QSEAL (legal person's qualified signature) with a Commitment Type of #proofOfCreation.
- The QSEAL (without the contract documents) is transmitted to the ASPSP and enters the Decoupled SCA procedure.

PSU performs SCA



- The QSEAL is downloaded to the SCA app of the PSU by the ASPSP.
- The QSEAL contains a reference to each element of the contract, together with a brief summary that is displayed to the PSU.
- When ready to approve, the PSU countersigns the QSEAL with a Commitment Type of #proofOfApproval. An electronic signature is created using the PSU's SCA credentials.
- The ASPSP verifies the PSU's signature and transmits the SCA proof to the TPP.

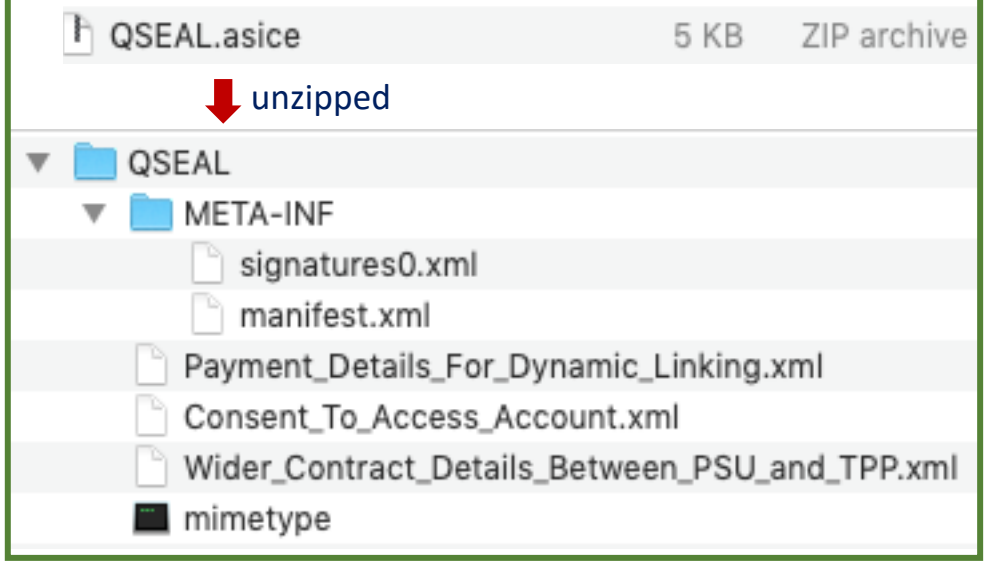
TPP embeds SCA & Initiates



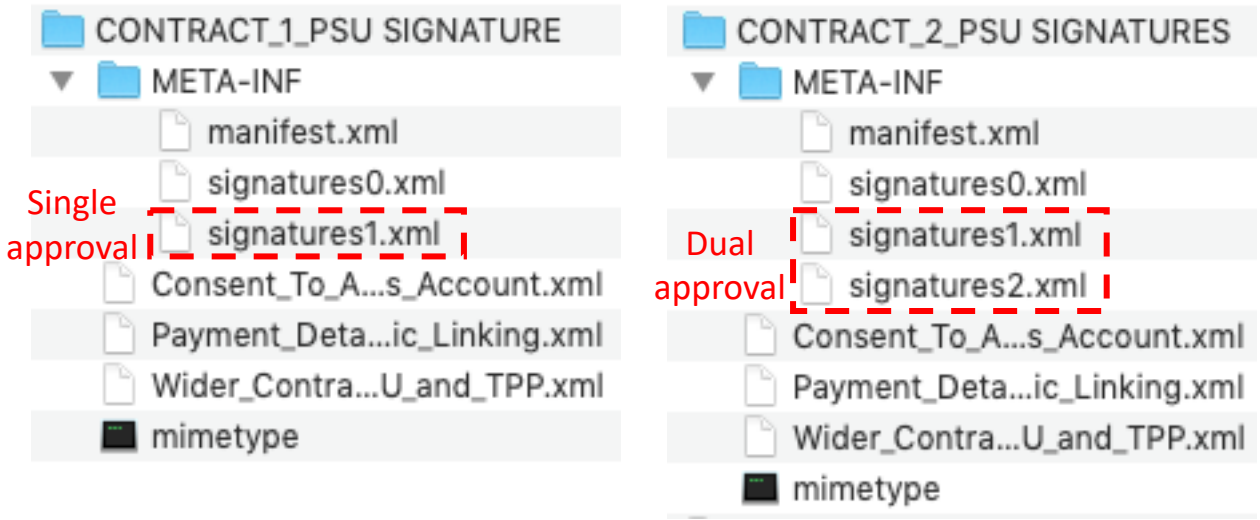
- The TPP requests the list of accounts, embedding SCA proof. The SCA proof includes the PSU's signature and the account consent element of the contract.
- The PSU selects the debit account and the TPP initiates a payment order, embedding the SCA proof. The SCA proof includes the PSU's signature and the payment consent element.
- The TPP packages the signatures and documents together into an Associated Signature Container (ASiC). This is sharable with and verifiable by the PSU (3rd party tool).

The SCA proof is packaged into an Associated Signature Container (ASiC). The TPP then embeds a subset of the SCA elements in account access and payment requests.

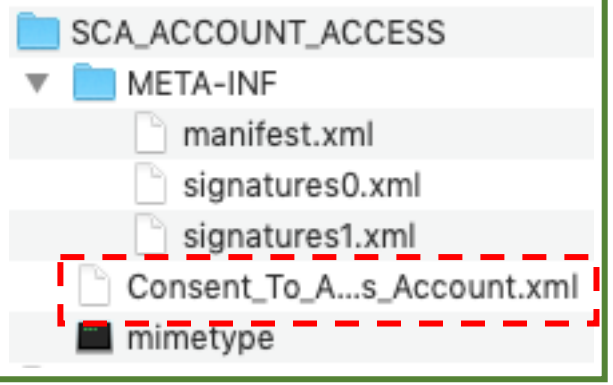
1. The TPP's QSEAL



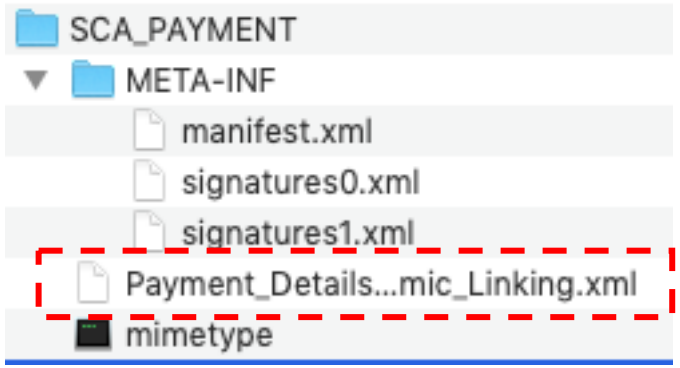
2. The Signed Contract



3. Embedded SCA for account access



4. Embedded SCA for payment initiation



Contents of the TPP's QSEAL - signatures0.xml (1 of 2)

In an XML Advanced Electronic Signature (XAdES) format

```
<?xml version="1.0" encoding="utf-8"?>
<asic:XAdESSignatures xmlns:asic="http://uri.etsi.org/02918/v1.2.1#">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="1566738789700">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference Id="Wider_Contract_Details_Between_PSU_and_TPP" Type="" URI="Wider_Contract_Details_Between_PSU_and_TPP.xml">
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>vw0aHj6xvbaPiDzgWuO75wW43tMJuxNZ6+tfmqdsd3U=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference Id="Consent_To_Access_Account" Type="" URI="Consent_To_Access_Account.xml">
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>a3w72w7XH4dghqFqCg89jdj+e8CqBWEqapbLX4gjJoE=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference Id="Payment_Details_For_Dynamic_Linking" Type="" URI="Payment_Details_For_Dynamic_Linking.xml">
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>BOTCh7mO5+Dn8LZ8ATmhcQ6wDGcUB/VZ75r7WPRtg2Q=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#1566738789700-SignedProperties">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>r3TjyRyZw4Ry172ExIPjlD5b+xYjXc2Cf7/rurVhRnY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue Id="1566738789700-SignatureValue">BUDlR7ssaxAeles0k9W5uiHsGH9y3GNLuCQwKBvgT++qGUQV75LW1l1J/yyRg/87pmS/Nn3Y2B
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>MIIDPzCCAicCAQswDQYJKoZIhvcNAQELBQAwcTELMAkGA1UEBhMCSVQxDDAKBgNVBAgTA1RwUzEMMAoGA1UEBxMDVHBMMQwwCgY
            </ds:X509Data>
        </ds:KeyInfo>
```

Hash value of each contract element

The TPP's signature

The TPP's QSEAL Certificate

QSEAL (2 of 2)

Timestamp

Account access consent

Payment consent

#proofOfCreation

```
        <ds:Object>
            <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#1566738789700">
                <xades:SignedProperties Id="1566738789700-SignedProperties">
                    <xades:SignedSignatureProperties>
                        <xades:SigningTime>2019-08-25T13:13:09.738Z</xades:SigningTime>
                        <xades:SigningCertificateV2>
                            <xades:Cert>
                                <xades:CertDigest>
                                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                    <ds:DigestValue>pm4t+n8RVl74NeYCvCmCJOhNJLM=</ds:DigestValue>
                                </xades:CertDigest>
                                <xades:IssuerSerialV2>MHowdaRzMHExCzAJBgNVBAYTAklUMQwwCgYDVQQIEwNUcFMxDDAKBgNVBAcTA1RwTDEMMAoGA1UEChMDVHB
                            </xades:Cert>
                        </xades:SigningCertificateV2>
                    </xades:SignedSignatureProperties>
                    <xades:SignedDataObjectProperties>
                        <xades:DataObjectFormat ObjectReference="#Wider_Contract_Details_Between_PSU_and_TPP">
                            <xades:Description>The terms and conditions of the contract between XYZ Ltd and Pete PSU</xades:Description>
                            <xades:MimeType>text/xml</xades:MimeType>
                        </xades:DataObjectFormat>
                        <xades:DataObjectFormat ObjectReference="#Consent_To_Access_Account">
                            <xades:Description>Grant XYZ Ltd access to my accounts</xades:Description>
                            <xades:MimeType>text/xml</xades:MimeType>
                        </xades:DataObjectFormat>
                        <xades:DataObjectFormat ObjectReference="#Payment_Details_For_Dynamic_Linking">
                            <xades:Description>Approve a payment of €75 to XYZ Ltd</xades:Description>
                            <xades:MimeType>text/xml</xades:MimeType>
                        </xades:DataObjectFormat>
                        <xades:CommitmentTypeIndication>
                            <xades:CommitmentTypeId>
                                <xades:Identifier>http://uri.etsi.org/01903/v1.2.2#ProofOfCreation</xades:Identifier>
                                <xades:Description>This indicates that the signature represents proof of creation</xades:Description>
                            </xades:CommitmentTypeId>
                            <xades:AllSignedDataObjects/>
                        </xades:CommitmentTypeIndication>
                    </xades:SignedDataObjectProperties>
                </xades:SignedProperties>
                <xades:UnsignedProperties>
                    <xades:UnsignedSignatureProperties>
                        <xades:CertificateValues>
                            <ds:EncapsulatedX509Certificate Id="S0-CA-CERT">MIIDdTCCAl0CAQowDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAklUMREwD
                        </xades:CertificateValues>
                    </xades:UnsignedSignatureProperties>
                </xades:UnsignedProperties>
            </xades:QualifyingProperties>
        </ds:Object>
    </ds:Signature>
</asic:XAdESSignatures>
```

Contents of PSU's SCA - signatures1.xml

In an XML Advanced Electronic Signature (XAdES) format

The PSU countersigns the TPP's QSEAL - signatures0.xml

#proofOfApproval

```
<?xml version="1.0" encoding="utf-8"?>
<asic:XAdESSignatures xmlns:asic="http://uri.etsi.org/02918/v1.2.1#">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="1567327544346">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha2
            <ds:Reference Id="signatures0" Type="" URI="META-INF/signatures0.xml">
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>j7ZMxFyO6Qcma1LaH8xXdyIlfwtnLedB673Dnm4g77o=</ds:Di
            </ds:Reference>
            <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#1
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256
                <ds:DigestValue>k50w26eCLelby8b76OYZ6nK4U7hfitBLhYKTNp/l9gc=</ds:Di
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue Id="1567327544346-SignatureValue">xGWTmMKnYf/Il6F8mnWyHI
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>MIIDnzCCAoegAwIBAgIEOx0b7TANBgkqhkiG9w0BAQsFADB
            </ds:X509Data>
        </ds:KeyInfo>
        <ds:Object>
            <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3
                <xades:SignedProperties Id="1567327544346-SignedProperties">
                    <xades:SignedSignatureProperties>
                        <xades:SigningTime>2019-09-01T08:45:44.000Z</xades:SigningT
```

```
                    <xades:SigningCertificateV2>
                        <xades:Cert>
                            <xades:CertDigest>
                                <ds:DigestMethod Algorith="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <ds:DigestValue>Fnu9LkLxL0h CA6brcaqY9mVnc=</ds:DigestValue>
                            </xades:CertDigest>
                            <xades:IssuerSerialV2>MH0wdaRzMHEx AJBgNVBAYTAkdCMREwDwYDVQQIDAhDaGVzaGly
                        </xades:Cert>
                    </xades:SigningCertificateV2>
                </xades:SignedSignatureProperties>
                <xades:SignedDataObjectProperties>
                    <xades:DataObjectFormat ObjectReference="#signatures0">
                        <xades:Description>Signature file to countersign</xades:Description>
                        <xades:MimeType>text/xml</xades:MimeType>
                    </xades:DataObjectFormat>
                    <xades:CommitmentTypeIndication>
                        <xades:CommitmentTypeId>
                            <xades:Identifier>http://uri.etsi.org/01903/v1.2.2#ProofOfApproval</xades:I
                        </xades:CommitmentTypeId>
                        <xades:AllSignedDataObjects/>
                    </xades:CommitmentTypeIndication>
                </xades:SignedDataObjectProperties>
            </xades:SignedProperties>
        </xades:QualifyingProperties>
    </ds:Object>
</ds:Signature>
</asic:XAdESSignatures>
```