



# Quali-Sign

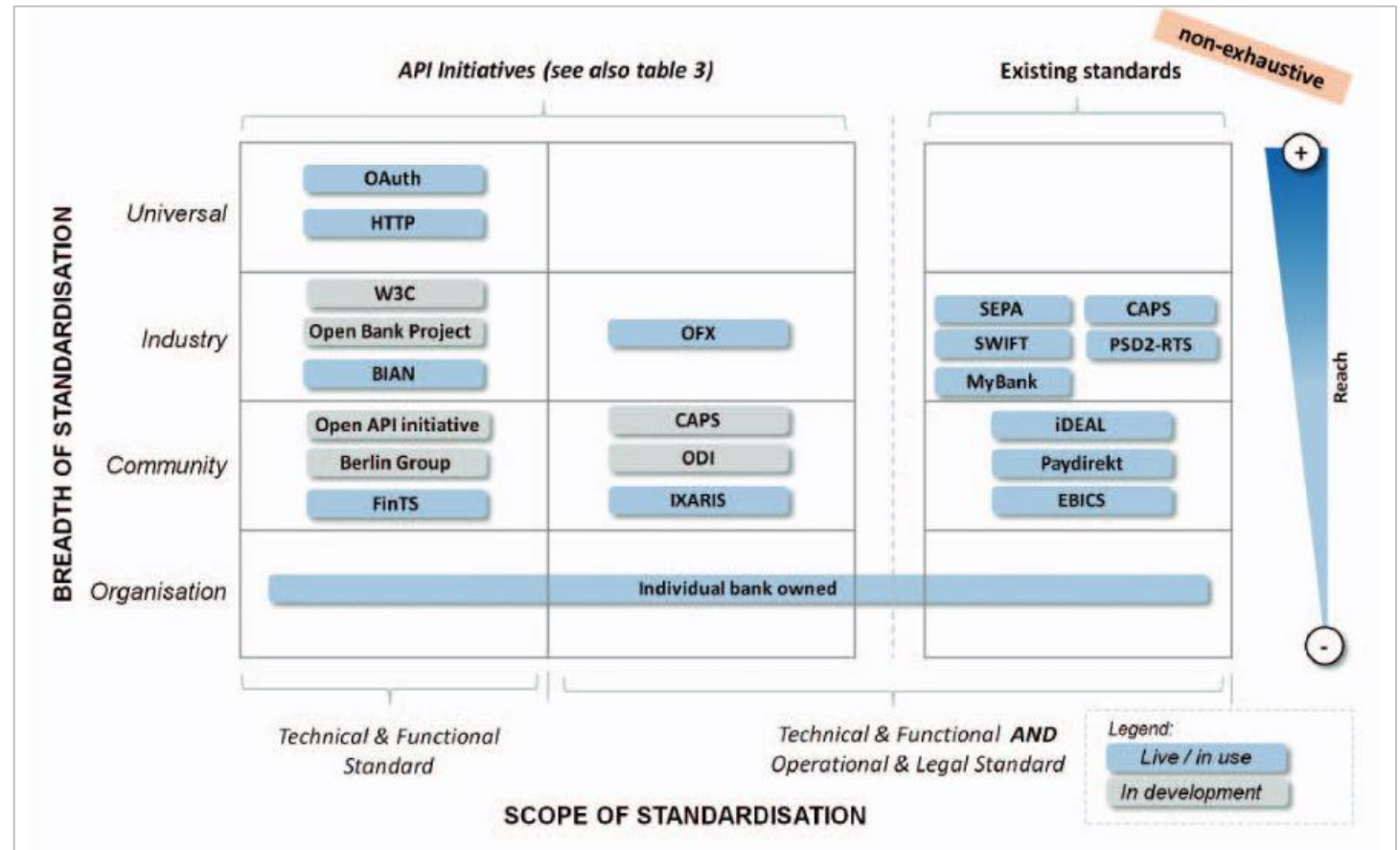
## Gap Analysis between EBICS and eIDAS.

Michael Adams

30<sup>th</sup> January 2017

# PSD2: Regulatory Technical Standards on SCA and CSC

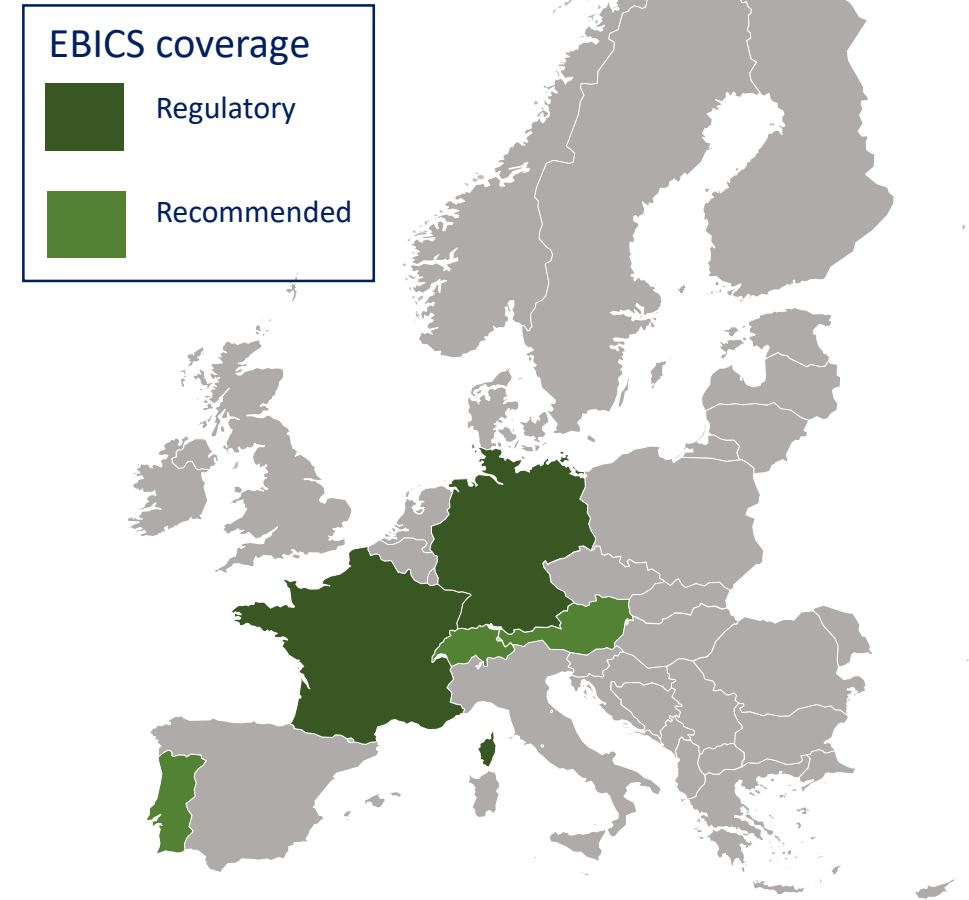
- ◆ To meet the PSD2 requirement for SCA, respondents to the EBA's consultation paper suggested a greater alignment with eIDAS.
- ◆ Which of the (International / European) open communication standards is the closest fit to eIDAS e-Signatures?



Source: Understanding the business relevance of Open APIs and Open Banking for banks  
 Information Paper, EBA Working Group on Electronic Alternative Payments, Version 1.0 May 2016

# EBICS: Electronic Banking Internet Communication Standard

- ◆ A common standard for banks and customers, based on HTTP(S) and XML.
- ◆ A European standard: The EBICS SCRL is responsible for the advancement and maintenance of the EBICS standard. Countries can join the EBICS SCRL.
- ◆ Supports exchange of ISO20022 format messages.
- ◆ Highly secure: Extensive use of cryptographic functions for encryption and digital signatures. Plus:
  - ◆ Support for X.509 certificate authority issued certificates.
  - ◆ Standard API's to initialize and manage users, including certificate exchange.
  - ◆ Centralized management of customer and user entitlements.
  - ◆ In built entitlements validation and authorisation workflow.
- ◆ An open standard: Includes a detailed specification.
- ◆ Turn-key EBICS software is available from established vendors.



# Gap Analysis : EBICS & eIDAS

Cryptographic Electronic Signatures	✓
Qualified Certificates (X.509)	✓
Qualified Trust Service Provider (Certificate Authority)	✓
Qualified Signature Creation Device (e.g. smartcard)	✓
Advanced / Qualified Electronic Signatures	✗



# EBICS

## Order Signature Data

```
<?xml version="1.0"?>
<UserSignatureData xmlns="http://www.ebics.org/S001" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.ebics.org/S001
http://www.ebics.org/S001/ebics_signature.xsd">
  <OrderSignatureData>
    <SignatureVersion>A005</SignatureVersion>
    <SignatureValue>
RqUZ1W/8xtzGhaBNxWHLAcjVYH9WezOK7cRQs24462q88X6DR66Kebx8WB2x+LZMrAy5WqHxx3IXamiqqkAepWgpsaT1U52yVt
jpLdZU7iMTLAjOjvkGEt0BDBX3fz24da9gL1TJCwU1j4wEB18Czu7+cdsZ5SfNBSn47qQm2dv+dt8IdSP97fXxIBDuwnD+TzYr
1GmcgRloV/Rdv/4Ci6YXScN1Tt+hSCp7A/P12PqeO6kgvCwpCzdhr2vFTulu0/O1Hv5H13ZFmdcye9EFPYRdH3mJsL8xu8HaAd
vibGfGbUj4bc2j+y8zjLSXemqGR5QPhaK5QJKWeY1PN1v1Cg==</SignatureValue>
    <PartnerID>TESTCORPB</PartnerID>
    <UserID>MADAMS5X</UserID>
  </OrderSignatureData>
</UserSignatureData>
```

Version of signature:  
A004, A005 or A006

Signature

User & organisation  
identifiers

# Proposed Enhancements to EBICS v 3.0

The image shows an XML snippet for EBICS v 3.0. It contains a `<UserSignatureData>` element with several sub-elements. A green box labeled "1) New signature version" points to the `<SignatureVersion>A005</SignatureVersion>` element. Another green box labeled "2) Replace with Advanced Electronic Signature" points to the `<SignatureValue>` element, which contains a long base64-encoded string. The XML is as follows:

```
<?xml version="1.0"?>
<UserSignatureData xmlns="http://www.ebics.org/S001" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.ebics.org/S001
http://www.ebics.org/S001/ebics_signature.xsd">
  <OrderSignatureData>
    <SignatureVersion>A005</SignatureVersion>
    <SignatureValue>
RqUZ1W/8xtzChaBNxWHLAcjVYH9WezOK7cRQs24462q88X6DR66Kebx8WB2x+LZMrAy5WqHxx3IXamiqqkAepWgpsaT1U52yVt
jpLdZU7iMTLAjOjvkGEt0BDBX3fz24da9gL1TJCwU1j4wEB18Czu7+cdsZ5SfNBSn47qQm2dv+dt8IdSP97fXxIBDuwnD+TzYr
1GmcgRloV/Rdv/4Ci6YXScN1Tt+hSCp7A/P12PqeO6kqvCwpCzdhr2vFTulu0/O1Hv5H13ZFmdcye9EFPYRdH3mJsL8xu8HsAd
vibGfGbUj4bc2j+y8zjLSXemqGR5QPhaK5QJKWeY1PN1v1Cg==</SignatureValue>
    <PartnerID>TESTCORPB</PartnerID>
    <UserID>MADAMS5X</UserID>
  </OrderSignatureData>
</UserSignatureData>
```

1. Define new signature version , e.g. A007.
  - ◆ Note: For the DataDigest to correspond with the DigestValue within the Advanced Electronic Signature, this must be calculated without removing operating system reserved characters.
2. Insert an (e.g. encoded) Advanced Electronic Signature within the SignatureValue
3. Store MimeTypes within the new EBICS BTF structure