Quali-Sign Ltd
www.quali-sign.com

EBICS Change Requests

Michael Adams
+44 (0) 7808 203856

13th July 2016

Table of Contents

1 HAA Order

Short description of the problem

The HAA order provides a list of download order types where new data is available for collection.

Where FileFormat is used, with the corresponding FDL order type, the HAA response does not identify the specific FileFormats with new download data available

```
<HAAResponseOrderData >
  <OrderTypes>FDL FDL FDL</OrderTypes>
</HAAResponseOrderData>
```

Description of the solution

A FileFormat tag should also be included

1.1 EBICS Working Group Response

HAA is used in Germany by many clients.

The list of order types represents all orders for whom anything is available on the bank server in the moment of HAA-Request. We will not change this, but in the future, the list of order types will be replaced by the BTF structure (0..N times) - hence no list is the responded but a structured overview.

It will be usable in all EBICS countries as BTF is standardised from new version

2 HTD / HKD Order UsageOrderTypes

Short description of the problem

The HTD and HKD orders include an optional <UsageOrderTypes> tag under <AccountInfoType>. If this tag is included, it restricts the account to be used with only the order types that are listed

When FileFormat is used, with the corresponding FUL and FDL order types, the <UsageOrderTypes> tag does not identify the corresponding FileFormat

<UsageOrderTypes>FUL FUL FUL FDL FDL FDL</UsageOrderTypes>

This has the effect of blocking the account, because the usage orders cannot be identified.

Description of the solution

A FileFormat tag should also be included

2.1 EBICS Working Group Response

Similar to HAA - BTF-structure will be integrated.

3 HTD / HKD Order OrderInfo

Short description of the problem

In HTD and HKD orders, where accounts are specified under the <AccountInfoType> tag without the optional <UsageOrderTypes> tag, this indicated that the account has unrestricted permissions.

Under the <UserInfo> tag. Permissions can be granted to a user that are unrestricted, i.e. not specific to a single account. This is achieved by not including the <AccountID> tag under the <Permission> tag.

This works well for account related orders, such as a daily account statement or intra-day account report. However there is no way of identifying from the OrderInfo, whether a specific order/FileFormat is applicable to account permissions or not. For example, it does not make sense to apply account permissions to a payment status report.

I have observed the impact of this with both EBICS Client and EBICS Server implementations. The EBICS Client will link the order to accounts that are unrestricted. The EBICS Server requests account permissions to be applied. Neither make sense.

Description of the solution

Within the <OrderInfo> tag in HTD and HKD orders, include a true/false attribute that indicates whether a particular order is account related or not.

3.1 EBICS Working Group Response:

In HKD and HTD the account relation means a restriction.
If Account is empty there is no restriction.
From our point of view this is consistent to the fact that for technical
order types no account is mentioned.
France intends to use HKD and HTD in the future (after BTF is implemented)

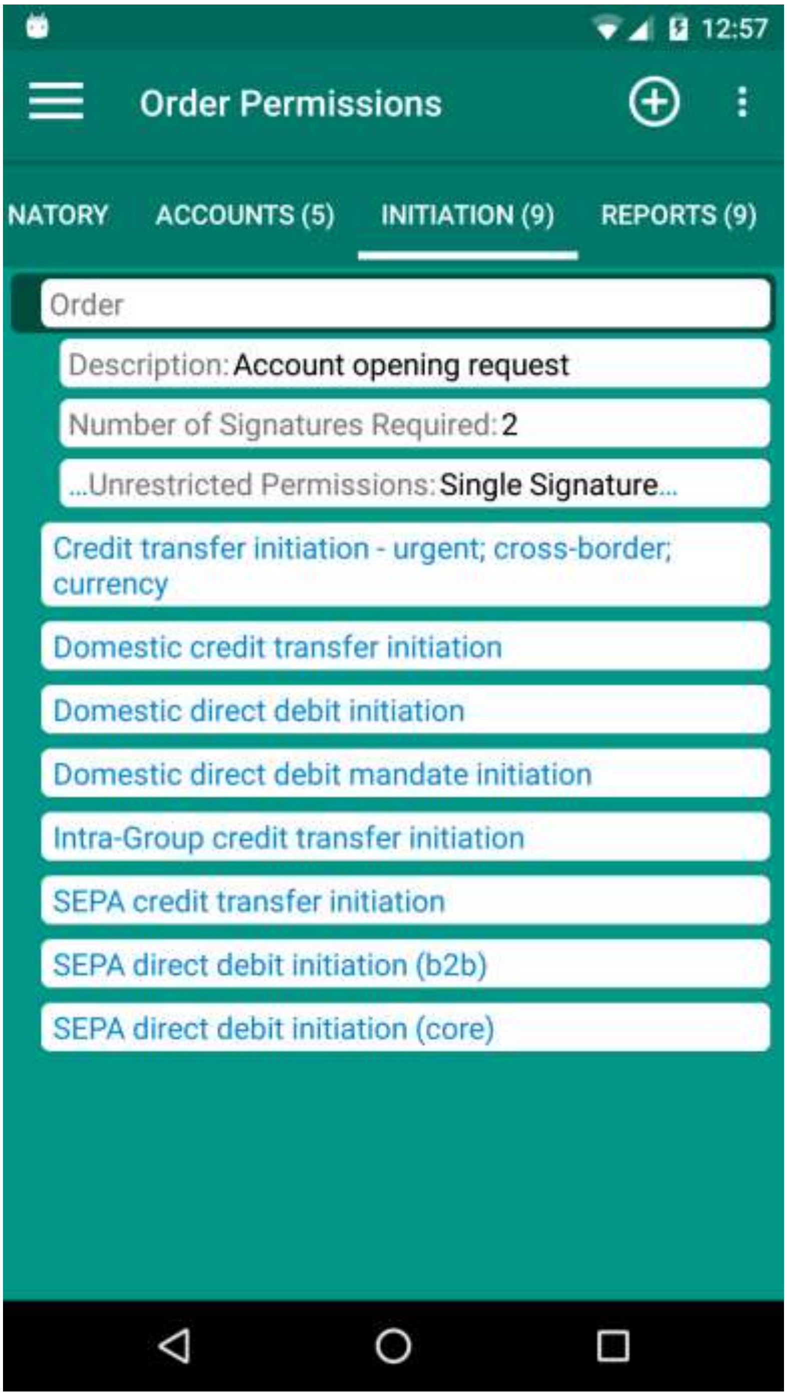
3.2 Further clarification of issue

If accounts are listed, what is the best practice with respect to unrestricted permissions?

There are two options:

a) Associate the unrestricted permissions with the account, so the user sees a full list of permissions against the account.
b) Do not associate the unrestricted permission with the account.

With the Quali-Sign Banking (QSB) app, I have opted for the first option. The following screenshots help to describe the issue



Order

Description: Account opening request

Number of Signatures Required: 2

...Unrestricted Permissions: Single Signature...

Credit transfer initiation - urgent; cross-border; currency

Domestic credit transfer initiation

Domestic direct debit initiation

Domestic direct debit mandate initiation

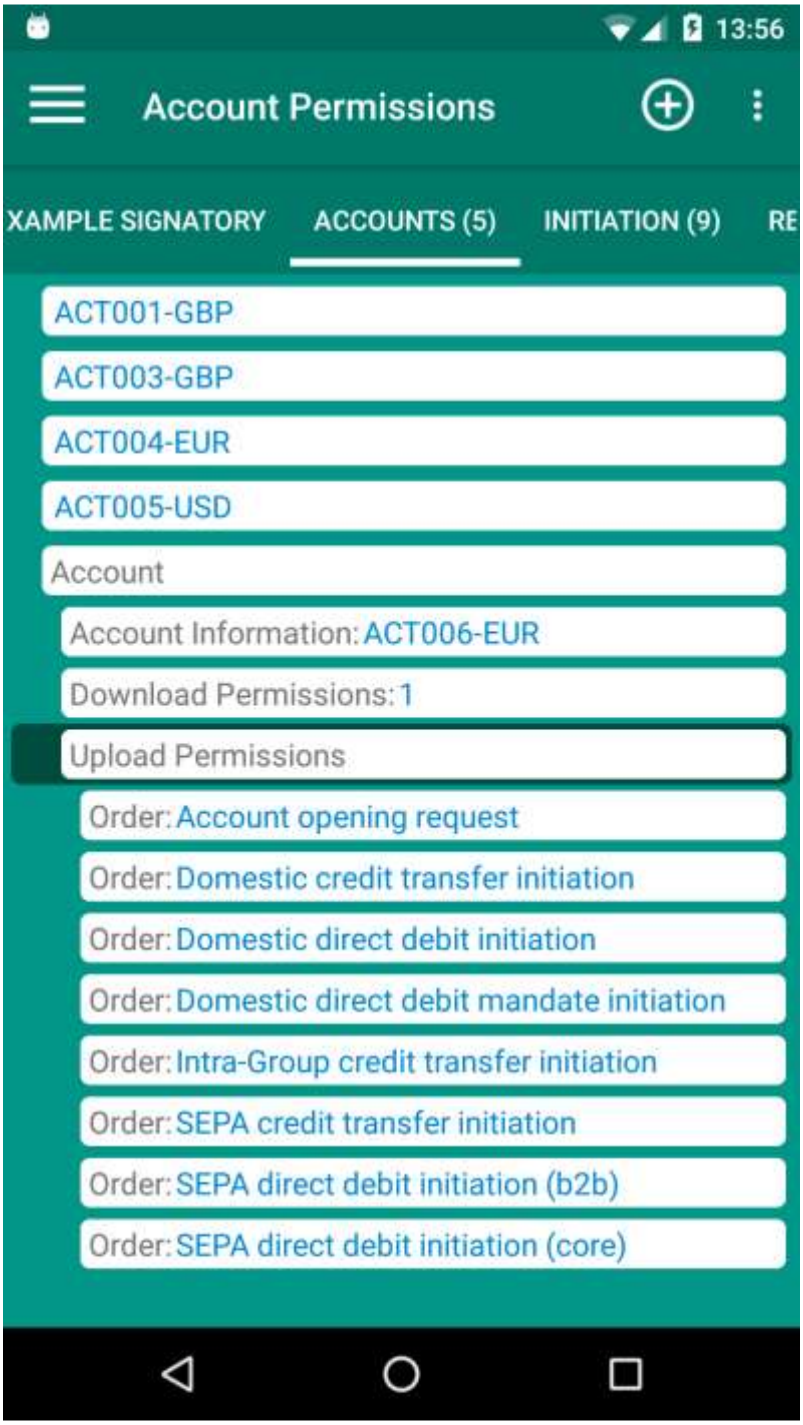
Intra-Group credit transfer initiation

SEPA credit transfer initiation

SEPA direct debit initiation (b2b)

SEPA direct debit initiation (core)

The above screenshot displays a list of all the initiation order types available to the user. The ‘Account opening request’ order is selected. It indicates that this order is unrestricted.



ACT001-GBP

ACT003-GBP

ACT004-EUR

ACT005-USD

Account

Account Information: ACT006-EUR

Download Permissions: 1

Upload Permissions

Order: Account opening request

Order: Domestic credit transfer initiation

Order: Domestic direct debit initiation

Order: Domestic direct debit mandate initiation

Order: Intra-Group credit transfer initiation

Order: SEPA credit transfer initiation

Order: SEPA direct debit initiation (b2b)

Order: SEPA direct debit initiation (core)

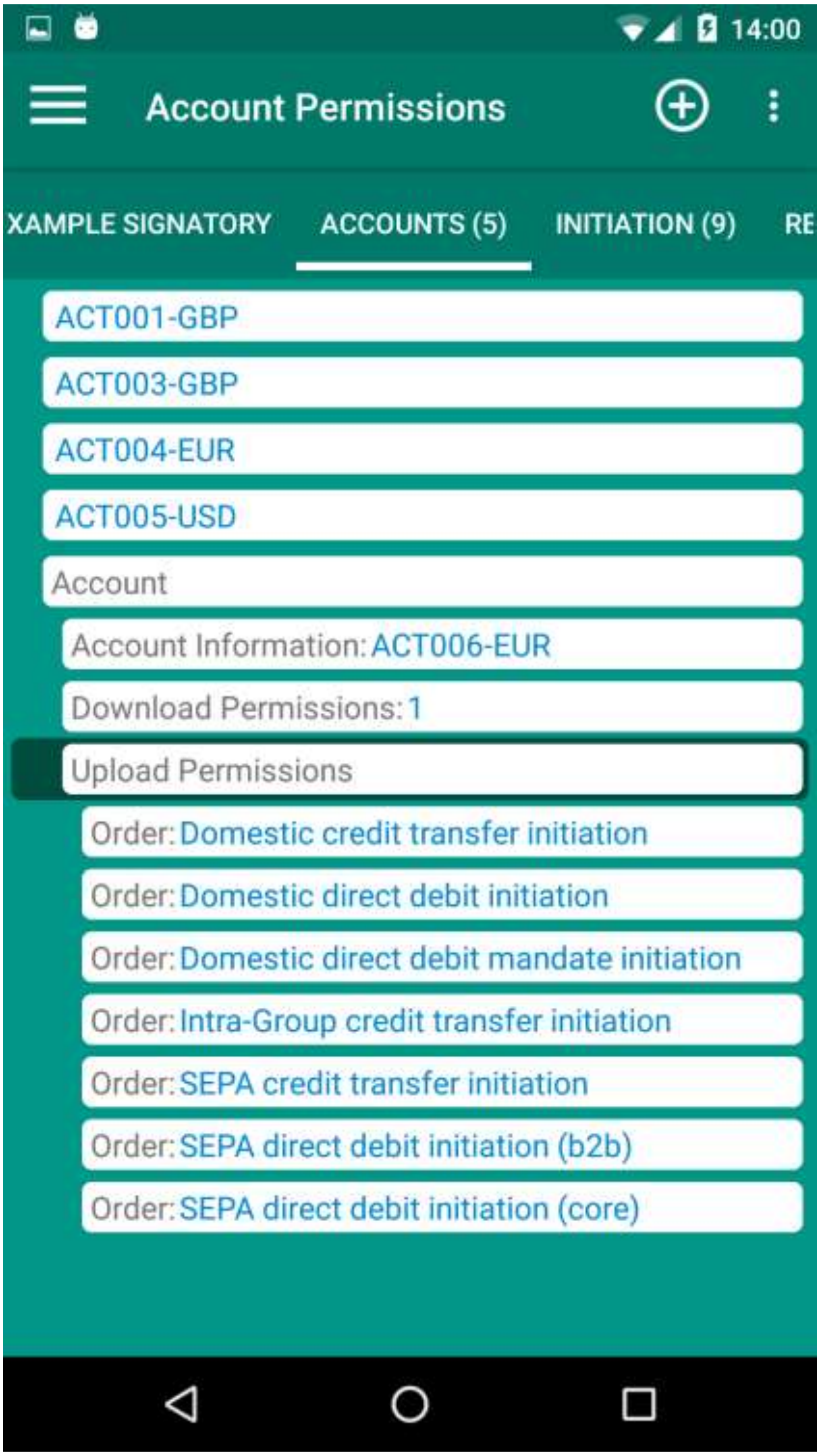
This screenshot displays a list of accounts that are available to the user. Account ‘ACT006-EUR’ is selected.

Below is the HKD, HTD XML that relates to ACT006-EUR. As you can see, the <UsageOrderTypes> tag is not present, this means that the account is unrestricted.

```
<AccountInfo Currency=\"EUR\" Description=\"Euro - all unrestricted\" ID=\"ACT006-EUR\">
  <NationalAccountNumber format=\"nnnnnnnnnnnn\" >555555566</NationalAccountNumber>
  <NationalBankCode format=\"nnnnnnnnn\">333333556</NationalBankCode>
  <AccountHolder>Account Holder Name 6</AccountHolder>
</AccountInfo>
```

Therefore all unrestricted order permissions can be associated to the account. Also displayed in the screenshot above is a list of ‘Upload Permissions’ that are associated with this account.

Please note that the ‘Account opening request’ order is included in this list. This does not make sense. It is not applicable to assign ‘Account opening request’ as a permission against an existing account.



ACT001-GBP

ACT003-GBP

ACT004-EUR

ACT005-USD

Account

Account Information: ACT006-EUR

Download Permissions: 1

Upload Permissions

Order: Domestic credit transfer initiation

Order: Domestic direct debit initiation

Order: Domestic direct debit mandate initiation

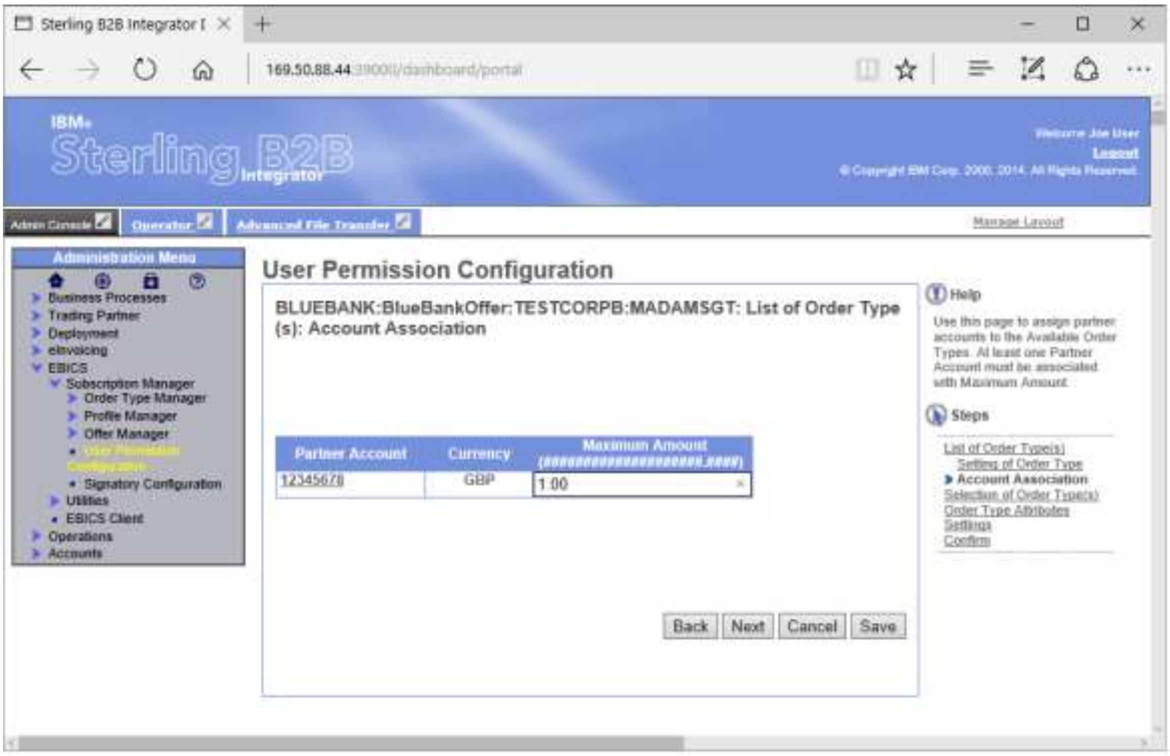
Order: Intra-Group credit transfer initiation

Order: SEPA credit transfer initiation

Order: SEPA direct debit initiation (b2b)

Order: SEPA direct debit initiation (core)

In the above screenshot the ‘Account Opening Request’ order is no longer included in the list. To achieve this, the ‘QSB’ app maintains a True/False flag that indicates whether an order is ‘Account Related’ or not.



User Permission Configuration

BLUEBANK:BlueBankOffer:TESTCORPB:MADAMSGT: List of Order Type (s): Account Association

Partner Account	Currency	Maximum Amount (####################.####)
12345678	GBP	1.00

Use this page to assign partner accounts to the Available Order Types. At least one Partner Account must be associated with Maximum Amount.

This same issue is also present in IBM's EBICS Server admin screens. When assigning user permissions, it asks for account and amount permissions to be supplied against all Upload Orders, even if these are not relevant.

Solution

When defining a new Upload Order (BTF?) on the EBICS Server, it would be beneficial to flag whether the new order is account related or not (i.e. account permissions can be assigned). By making this flag available to the user via HKD / HTD, this would also be beneficial to the EBICS Client.

4 HTD / HKD Order - Order Format

Short description of the problem

In the HTD and HKD orders, there is an optional <OrderFormat> tag within the <OrderInfo> tag. The EBICS specification (page 236) indicates this as a token, maxLength=8.

There does not appear to be a standard catalogue of Order Formats.

Banks are able to define Reserved Order Types. These are prefixed with X, Y or Z and are for bank-individual purposes and reserved between the bank and the customer.

When Reserved Order Types are used, it is difficult determine the file format of the order. The use of the <OrderFormat> tag appears to be the solution, but the lack of standards around definition of formats makes this difficult.

Also, likewise where FileFormat is used with the FUL and FDL order types, it is sometimes difficult to determine the format unless a pre-defined FileFormat pattern is used. For example 'pain.001.001.03.dct'.

Description of the solution

Publish a standard catalogue of formats and include an attribute in the <OrderFormat> tag, indicating whether the supplied value corresponds to a value in the catalogue or is proprietary.

4.1 EBICS Working Group Response

The order format element will be deleted in the next EBICS version. But: the Format will be a part of the BTF structure via an element called <MsgName> (there will be clear definition how to use it).

5 HTD / HKD Order – Country tag

Short description of the problem

I have observed that some EBICS server implementations include the full country name within the <PartnerInfo><AddressInfo><Country> tag, whereas other EBICS server implementations include a 2 digit ISO country code. Both are acceptable according to the Schema and the EBICS Specification

Description of the solution

Include an optional true/false attribute within the <Country> tag that indicates whether a valid 2 digit ISO code has been supplied.

5.1 EBICS Working Group Response

This tag will also be deleted in the next EBICS version. Instead of country tag there will be an element called <Scope> - for Scope we will define an external code list (list is defined and maintained by the EBICS SCRL) - hence the codes are well-defined, for example the two-letter country code if you follow the rules of a specific country (DE, FR ...) or a three-letter code for further

Scopes / markets (BGR = Berlin group, BIL =bilateral between two partners ...)

6 HTD / HKD Order – BankInfoType

Short description of the problem

The HTD and HKD orders include a <BankInfoType> tag. Page 225 of the EBICS Specification explains that this is a “Data type for bank information with regard to distributed signatures (order types HKD, HTD). I have tested distributed signatures with two different EBICS Servers. The use of this tag is not clear to me”

Description of the solution

Please provide more detail in the EBICS Specification on the use of the <BankInfoType> tag.

6.1 EBICS Working Group Response

Not discussed in detail. When updating HKD/HTD for BTF we can maybe act on you suggestion

7 HAC Order

Short description of the problem

I have observed that with two different EBICS Servers, information appears to be reported In a HAC response only once. In the case where a Partner has multiple users, the first user to call the HAC will receive the information, all subsequent users will not.

This is not ideal because the HAC provides further information on whether an order was in fact successful or not, which is not reported in an EBICS response. If a particular user uploads a file and receives an EBICS_OK response. It may be subsequently rejected and this is reported in the HAC. However if a different user downloads this information, the user that uploaded the file will not be provided with the reject information.

Description of the solution

Provide an optional attribute within the HAC request that allows a user to specify an OrderId. If the OrderId tag is supplied, only information corresponding to the order should be reported in the HAC. All activity that corresponds with this OrderId should be reported, regardless as to whether it has been reported before.

Each bank can decide how long historic information is available. For example 30 days.

7.1 EBICS Working Group Response:

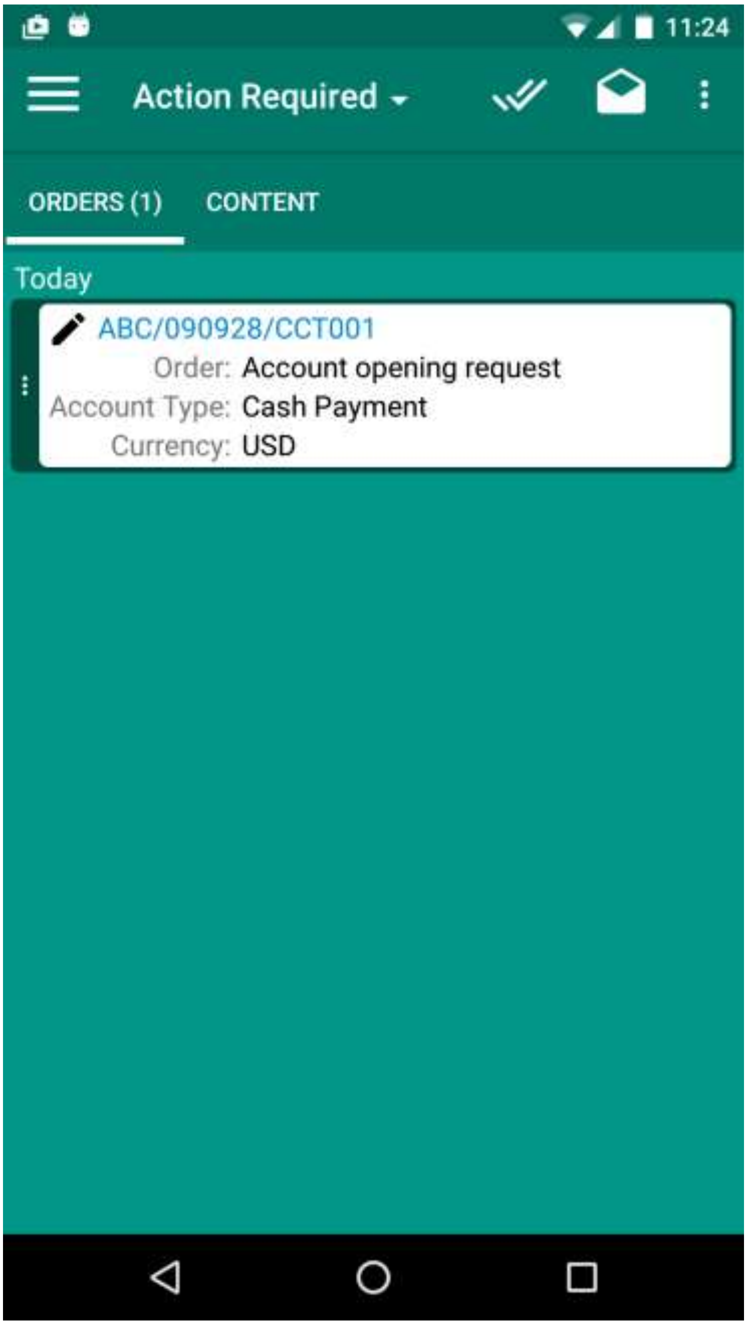
Not discussed - I assume that you proposal will not be accepted as HAC (and PTK as well - tzhis is the previous acknowledgement in Germany) is defined for the complete view and is also for legal reasons in Germany (completeness of processing of all EBICS actions). I will keep track on this in one of our next meetings / discussions

7.2 Further clarification of issue

From what you have described above, the HAC should really not be available to all users, it should be used by a single 'super' user who can keep track of all activity. As soon as HAC is available to more than one user, a single “complete view” is not possible.

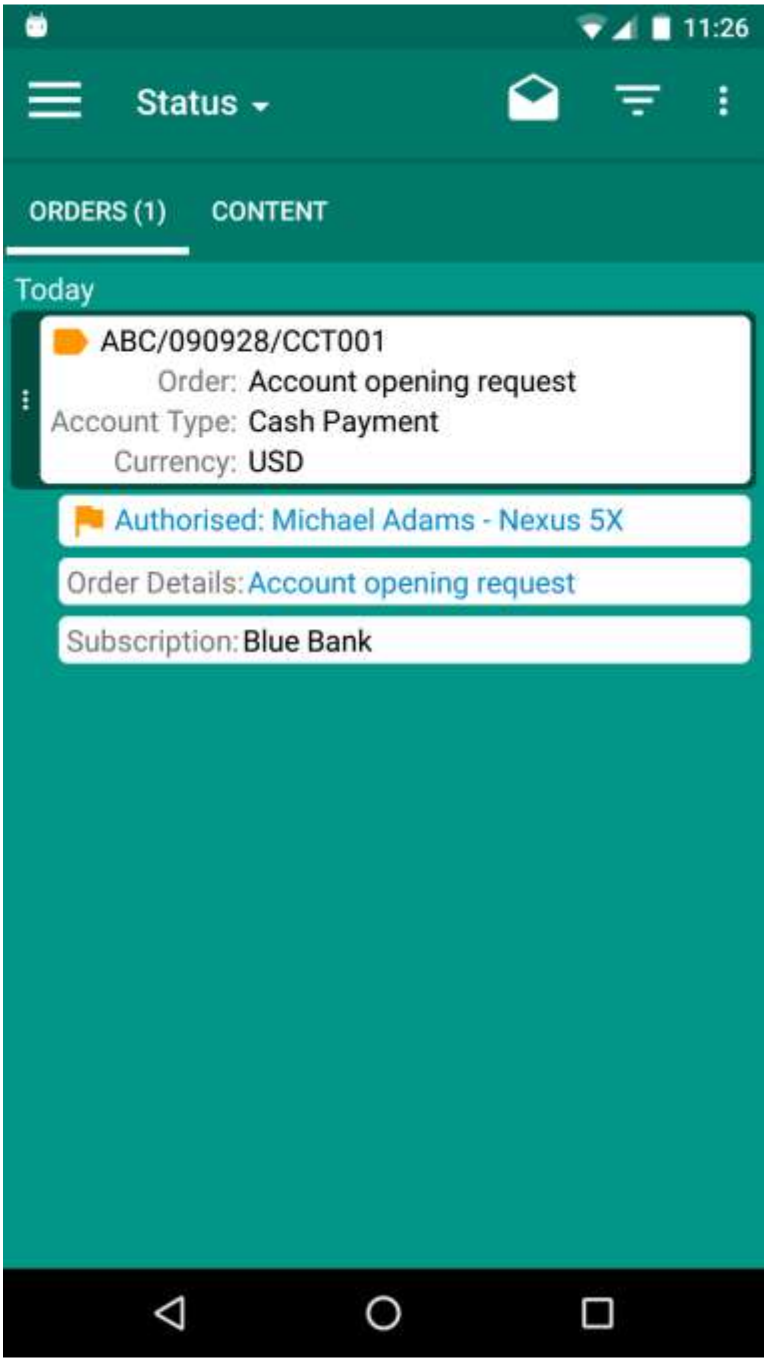
The problem with restricting user access to HAC is that the user may not be aware of the EBICS server rejecting an upload after the EBICS_OK has been received. For example the upload may be rejected because of a problem with the order data signature. This is validated after the EBICS_OK is returned.

I have included the following screenshots to further elaborate on this issue



ABC/090928/CCT001
Order: Account opening request
Account Type: Cash Payment
Currency: USD

This screenshot shows an ‘Account opening request’ order that is awaiting signatures from personal authorisation users.



Today

ABC/090928/CCT001
Order: Account opening request
Account Type: Cash Payment
Currency: USD

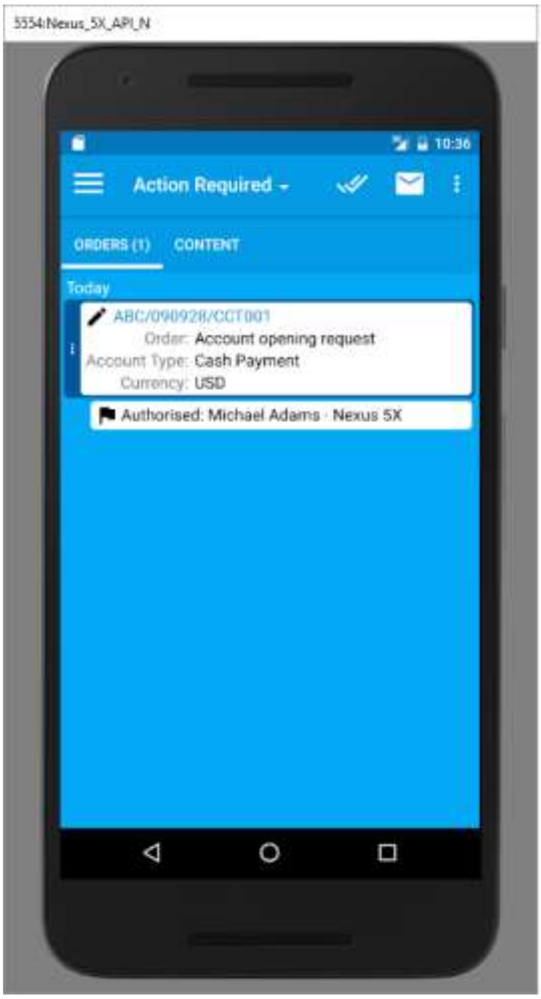
Authorised: Michael Adams - Nexus 5X

Order Details: Account opening request

Subscription: Blue Bank

Once the first signer (in this case Michael Adams – Nexus 5X), has signed the order, the user can continue to track the status of the order.

After the user approves the order (via HVE), the app calls HAC to confirm that the user signature was accepted.



5554:Nexus_5X_API_N

10:36

Action Required

ORDERS (1) CONTENT

Today

ABC/090928/CCT001

Order: Account opening request

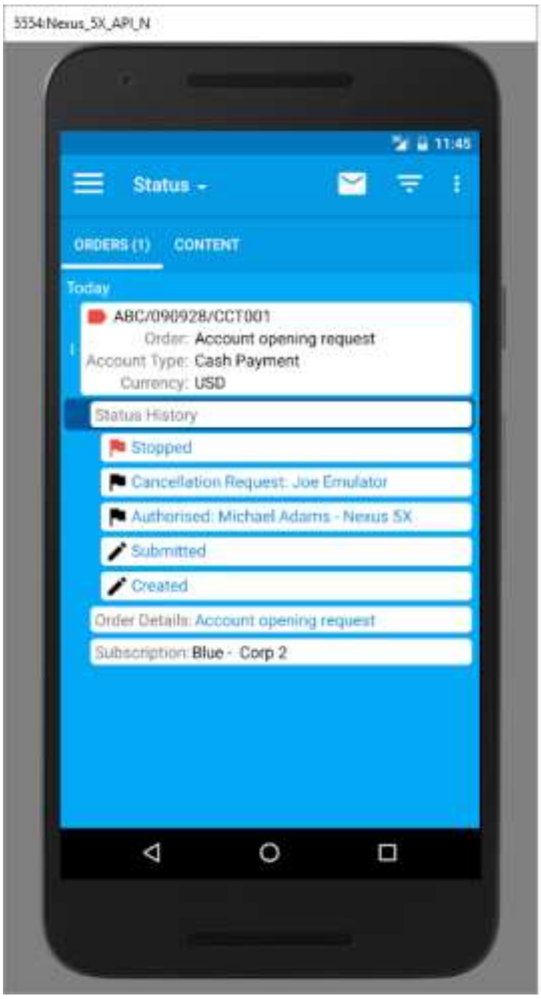
Account Type: Cash Payment

Currency: USD

Authorised: Michael Adams · Nexus 5X

A second user can see that the order has been authorised already by ‘Michael Adams – Nexus 5X’

This second user decides to cancel the order, via ‘HVS’.



Today

ABC/090928/CCT001
Order: Account opening request
Account Type: Cash Payment
Currency: USD

Status History

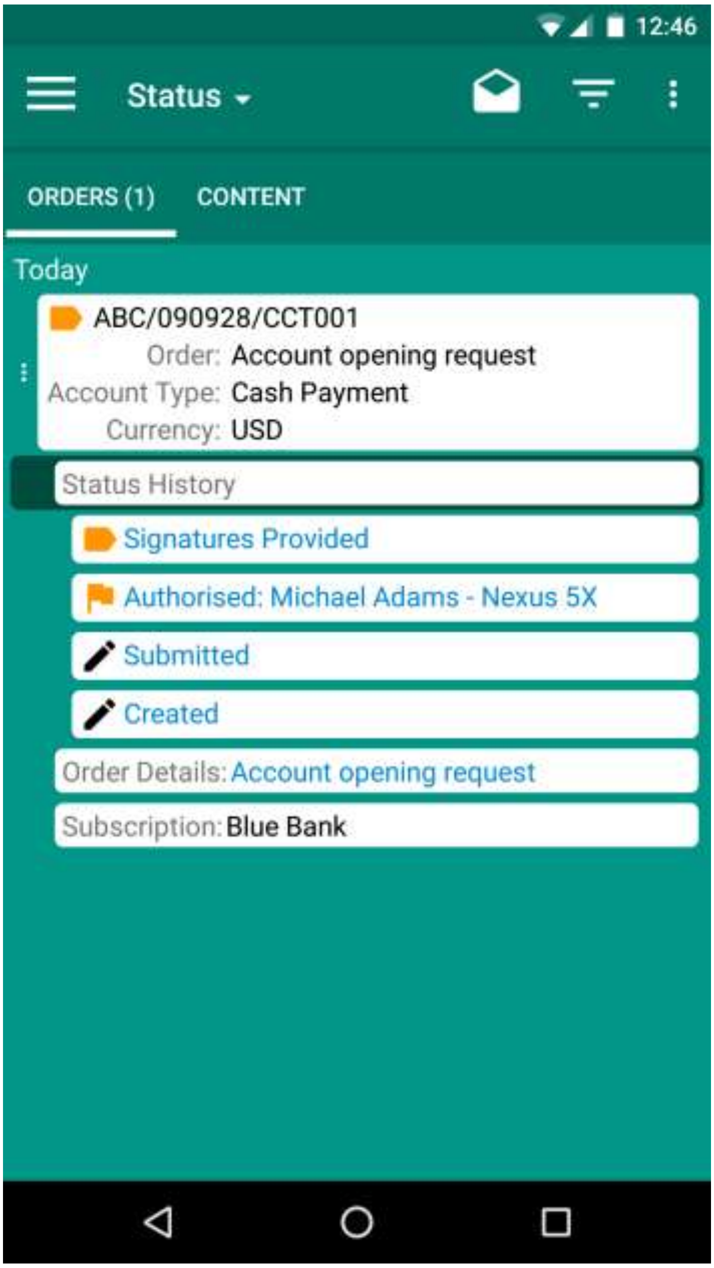
- Stopped
- Cancellation Request: Joe Emulator
- Authorised: Michael Adams - Nexus 5X
- Submitted
- Created

Order Details: Account opening request

Subscription: Blue - Corp 2

The app calls HAC after HVS to confirm that the order has been stopped.

The second user can clearly see that their cancellation request was successful.



Today

ABC/090928/CCT001
Order: Account opening request
Account Type: Cash Payment
Currency: USD

Status History

- Signatures Provided
- Authorised: Michael Adams - Nexus 5X
- Submitted
- Created

Order Details: Account opening request

Subscription: Blue Bank

However, the first user has no way of knowing that the second user cancelled the order. All they know is that the order is no longer in the VEU. It may have been approved or cancelled. It is not possible for the first user to determine this. This is because the HAC confirmation that the order was stopped was already downloaded by the second user. It is no longer available to the first user.

8 VEU – History

Short description of the problem

When an order exits VEU processing due to being forwarded or cancelled, there is no further information available on the order. Therefore it is difficult to confirm whether an order was forwarded or stopped (i.e. cancelled) and which personal authorisation users undertook the action.

Description of the solution

Provide an additional VEU order, with the ability to supply an OrderId in the request that then returns a summary of the order's status. A similar level of information to HVZ should be supplied (i.e. originator and signer information), together with an indication of whether the order was forwarded or stopped (cancelled).

Each bank can decide how long historic information is available. For example 30 days.

8.1 EBICS Working Group Response:

There is currently no requirement in Germany for such a service (and in France the VEU is still not used)

8.2 Further clarification of issue

With reference to the screenshots in the section above, if there was a way that VEU history could be made available, this would remove the need for every HAC entry to be downloaded by every user (if this was possible) in order for all users to determine whether the order was forwarded or stopped. It would be much more efficient for the EBICS Clients to have access to an order's VEU history rather than attempting to process a large amount of HAC activity.

9 Initialization with a Certificate Signing Request

Short description of the problem

X.509 is currently optional but will become mandatory. When X.509 is used, for personal authorisation users, an X.509 certificate issued by an X.509 certificate authority, must be supplied within the INI order.

This works fine with physical tokens (e.g. USB key / Smartcard), but is more challenging when keys are generated (for example locked into the hardware of a mobile phone or tablet).

Description of the solution

Provide an additional initialization order (as an alternative to INI) that will accept a ‘Certificate Signing Request’ instead of an issued certificate. This should be available where the bank is prepared to act as a certificate authority (Qualified Trust Service Provider).

This would allow EBICS to provide a standard means of transmitting the Certificate Signing Request to the bank.

The initialization letter should contain additional subject information relating to the certificate. This may also need to be signed in the presence of a bank official (see Article 24.1 of e-IDAS: Regulation on electronic identification and trust services for electronic transactions in the internal market).

An additional download order should also be defined to allow the user (once activated) to download a copy of their new CA issued certificate to their device. This will allow them to initialize with other institutions, via H3K.

9.1 Further clarification of issue

I believe this to be an important enhancement that would make the EBICS standard more applicable to the use of mobile devices to generate eIDAS compliant ‘Qualified Electronic Signatures’ (QES).

A demonstration is available at http://www.quali-sign.com/banking.html that shows the process of initializing a user. It is currently necessary to initialize the user initially as a transport user in order to transmit the CSR. This would not be necessary if the user was able to be initialized with a CSR.

10 Other Partner Permissions

Short description of the problem

Where a user is assigned approval permissions on behalf of another partner, it is not clear how these permissions are shared with the user.

Description of the solution

Provide these permissions within HTD / HKD

10.1 EBICS Working Group Response

Not discussed in the workshop by reason of time

11 HVTResponseOrderData Summary Template

Short description of the problem

HVTResponseOrderData includes OrderInfo summary information. This is good for payments, but what about other order types that may benefit from summary information.

Description of the solution

Provide the ability to define a custom OrderInfo template that could replace the payments template

11.1 EBICS Working Group Response

Not discussed in the workshop by reason of time