Íslenskir staðlar

ÍST WA 316:2022

Gildistaka: 2022-02-15

ICS. 3.060

Vinnustofusamþykkt -

Tæknilegar upplýsingar

Workshop Agreement -

Technical Guidelines

Íslenskir staðlar

ÍST WA 316:2022

Participants in TN-FMÞ Financial services (is. Fjármálaþjónusta) During the development of ÍST TS 316 document.

Name:	Company / organisation / association:
Árni Geir Valgeirsson	Íslandsbanki
Ásgeir Helgi Jóhannsson	Afl lögmenn
Atli Guðmundsson	Rapyd/Kortaþjónustan
Bergljót Kristinsdóttir	ICEPRO
Bjarni Þór Pálsson	RB
Björgólfur G Guðbjörnsson	Origo
Gísli Konráð Björnsson	Landsbankinn
Guðjón Karl Arnarson	RB
Guðmundur Jón Halldórsson	CTL
Halldór Vagn Hreinsson	Landsbankinn
Halldór Péturson	Fjármálaeftirlitið
Hermann Snorrason	Landsbankinn
Hjálmar Brynjólfsson	Seðlabanki Íslands
Hrannar Már Hallkelsson	Arion banki
Ingveldur Lárusdóttir	Landsbankinn
Ingibergur Sindri Stefnisson	Unimaze
Jóhannes Þór Ágústarson	Íslandsbanki
Kristinn Stefánsson	Arion banki
Markús Guðmundsson	Unimaze
Ólafur Tryggvason	Advania
Sigrún Gunnarsdóttir	WISE
Sigurður Gauti Hauksson	Alskil
Sigurður Másson	Advania
Styrmir Kristjánsson	Sjálfstæður
Sveinn G. Gunnarsson	Landsbankinn
Védís Ingólfsdóttir	Arion banki

ÍST WA 316:2022

Name:	Company / organisation / association:
Védís Sigurðardóttir	Landsbankinn
Sigurvin Sigurjónsson	KPMG

1. edition

Table of contents

ICS. 3.060

ÍST WA 316:2022

TODO

- ☐ Review list of final WA participants
- ☐ Double check endpoints, for IOBWS Payments and Accounts updates.
- ☐ Double check endpoints, for Claims final version.

Foreword

This IST workshop agreement was developed in accordance with “ÍST Reglur um tækniforskriftir, tækniskýrslur og vinnustofusamþykktir” (*e.* IST rules on Technical Specifications, Technical Reports and Workshop Agreements). It was agreed on 2021-X-X in a workshop by representatives of interested parties, approved and supported by IST following a public call for participation within TN-FMÞ, the FUT technical committee on financial services. It does not necessarily reflect the views of all stakeholders that might have an interest in its subject matter.

The Workshop Agreement (ÍST WA) was funded by Íslandsbanki, Arion banki and Landsbankinn. This ÍST WA is based on the results of the work of two workgroups TN-FMÞ-VH-1 Technical requirements and TN-FMÞ-VH-2 Business requirements.

The final text of ÍST WA-316 was submitted to IST for publication on 2021-X-X. It was developed as part of the agreement made by TN-FMÞ under the working group TN-FMÞ-VH7, and approved by:

- Arion banki (Atli Már Gunnarsson, Védís Ingólfsdóttir, Björn Ingi Björnsson. Kristinn Stefánsson, Eiríkur Haraldsson, Eiríkur Egilsson, Steinar Þorbjörnsson)
- Íslandsbanki (Halldór Vagn Hreinsson, Ingvi Rafn Guðmundsson, Snorri Jónsson, Jóhannes Þór Ágústarson, Snorri Karlsson,
  Stefán Orri Stefánsson, Frans Veigar Garðarson)
- Landsbankinn (Hermann Þór Snorrason, Jökull Huxley Yngvason, Ólafur Eiríksson, Halldóra G. Steindórsdóttir, Guðni Þ. Björgvinsson, Guðmundur Ólafsson, Gísli Konráð Björnsson)
- Alskil (Sigurður Gauti Hauksson)
- Uniconta (Þorsteinn Lemke)
- RB (Guðjón Karl Arnarsson, Halla Sigrún Árnadóttir)

ÍST WA-316 is not subject to any patent rights. As part of the IOBWS v3.0 Technical Specifications, the technical contracts are distributed under a Creative Commons Attribution 4.0 International Public Licens.

The Workshop participants have made every effort to ensure the reliability and accuracy of the technical and non-technical content of ÍST WA-315, but this does not guarantee, either explicitly or implicitly,

its correctness. Users of ÍST WA-316 should be aware that neither the workshop participants, nor IST can be held liable for damages or losses of any kind whatsoever which may arise from its application. Users of ÍST WA-316 do so on their own responsibility and at their own risk.

1 Introduction

This Workshop Agreement (TS) presents aspects of the preferred way to implement API service in IOBWS 3.0.

API interfaces enable various systems to interact with the financial resource. Example of such use cases are accounting systems, but others are provided in teh section on Use Cases.

The Icelandic banks together with RB (Clearing House of Iceland), Central Bank of Iceland, software companies, billing companies, fintech companies and other stakeholders within the TN FMÞ at the Icelandic Standards Council have maintained specifications on how the banks should conduct electronic interconnection in the construction of interfaces APIs. The first version of that standard was published in 2007 and was named IOBWS (Icelandic Online Banking Web Service). Six years later, version 2, IOBWS 2.0 of the standard was published. The work was developed to make corrections and upgrade to business operations that were not foreseen in the earlier standard. This document describes the partial results of the fifth phase of the third IOBWS project, IOBWS 3.0.

This document is based on the results from the working group of the TN-FMÞ-VH7.

ICS. 3.060

2 Scope

The technical specifications for individual aspects of the Icelandic Online Banking Web Services 3.0, (IOBWS3) do not address common implementation details. These guidelines will try to do address some cross cutting concerns related to authentication and authorization, as well as idempotency. As such they apply to the specifications in the following documents, and associated YAML definitions:

- TS 312:2021 Currency
- WA 310:2020 Domestic payments and deposits (Will become TS 310:2022)
- WA 311:2021 Debit and credit cards details and statements (new in IOBWS v3.0)
- TS 315 Claims (in draft) TS 31x Secondary Collection (not started)
- TS 314:2021 Documents
- TS 313:2021 Foreign Payments

It is the intention that the guidelines will be an evolving document, with new version issued as workshop agreements. Clarifications and changes can be suggested through issues on the Github site or with direct Pull Requests. All updates, similar to the maintenance of the technical specifications, will be funneled through Pull Requests as part of the regular work overseen by workgroup 7 (VH-7). It is expected they will then be released regularly by the working group TN-FMÞ-VH7.

3 Normative references, definitions, and symbols

3.1 Definitions

- **IOBWS 3.0** – This is the acronym of the third version of the Icelandic Open Banking Web Services project and its product.
- **FUT** is the IT sector council at Icelandic standards.
- **TN-FMÞ** - Technical committee on finance services, working under FUT.

4 Authentication Use Cases and Requirements

The API specifications for IOBWS reference OAuth2 based authorization, and reflects the NextGenPSD2 ancestry with occasional references to Strong Customer Authentication and consents.

Listing 4.1: IOBWS 3.0 full flows

```
17        * OAuth SCA Approach
18        The following items are not required. Optional for each bank to
              implement.
19        * Decoupled SCA Approach
20        * Embedded SCA Approach without SCA method
21        * Embedded SCA Approach with only one SCA method available
22        * Embedded SCA Approach with Selection of a SCA method
23
24        Not every message defined in this API definition is necessary for
              all approaches.
```

These guidelines further elaborate on the ways the most common use cases should be handled among all implementors and consumers of the APIs that adhere to the workshop agreement.

It is established that the usage of “Búnaðarskilríki” issued under Fullgilt Auðkenni as the current gold standard for authentication and they will continue to be supported as such. The usage of username and passwords in combination with X.509 certificates, as in the previous IOBWS specifications, is not longer supported.

Additionally, OpenID Code Flow with PKCE will be part of the common support to handle the various scenarios.

4.1 Main Use Cases

To harmonize technical expectations, some basic use cases are considered and the acceptance criteria should guide implementors towards selecting the correct solution.

4.1.1 Centralized Financial System

> As a **Financial System**, I want to connect to IOBWS 3.0 services so that I can e.g. manage Claims, initiate Payments, and fetch Account transactions in batches or directly on behalf of users.

Acceptance criteria:

1. Support for Búnaðarskilríki issued under Fullgilt Auðkenni, for authenticating and authorizing centralized software to act on behalf of organizational units.
2. Support for OIDC and, code flow with PKCE as the common denominator.
3. Support for online scenarios, where the organization authenticates the interactive employee that instigates the action.

4.1.2 On-premise System

> As **a user of an on-premise Financial System**, I want to be able to authorize the system to connect to IOBWS 3.0 services and manage Claims, initiate Payments and fetch Account transactions on my behalf in non-interactive sessions.

Acceptance criteria:

1. Support for OIDC and OAuth 2.0, code flow with offline_access, using MTLS to identify the client/server using Búnaðarskilríki issued under Fullgilt Auðkenni.

4.1.3 On-premise employee

> As a **company employee** I want to e.g. initiate payment instructions, create claims and interact with IOBWS 3.0 so that I can manage my day-to-day activities through e.g. the company ERP system.

Acceptance criteria:

1. Support for OIDC and OAuth 2.0, code flow with PKCE as the common denominator.
2. Support for user authentication with Qualified Certificates.

4.1.4 Financial Services

> As e.g. **an independent Accounting firm** offering services to multiple clients, I want to be able to access their accounts and products through IOBWS 3.0, so I can manage their financials and accounting.

Acceptance criteria:

1. Support for assuming multiple identities.
2. Support for OIDC and OAuth 2.0, code flow with PKCE as the common denominator.
3. Support for user authentication with Qualified Certificates.
4. The scopes should be known, based on the endpoints defined in IOBWS 3.0.

4.1.5 Financial Software as a Service

> As the IOBWS 3.0 **customer of a bank**, I want to be able to authorize SaaS software hosted in public clouds to act on my behalf, so I can allow the service to manage my financials and the products I have access to such as Claims.

Acceptance criteria:

1. This should address the scenario where companies offering e.g. Dynamics 365 or more custom apps need to act on behalf of bank customers.
2. Support for OIDC and OAuth 2.0, code flow with PKCE as the common denominator.
3. Support for user authentication with Qualified Certificates.

4.1.6 Software Vendor

> As a **Software Vendor** providing Custom, COTS, or SaaS applications that my clients use to accesses IOBWS 3.0, I want to be able to target common authentication behavior as part of the technical standard offered by all the banks, so that I do not have to implement and test against multiple subtly different endpoints.

Acceptance criteria:

1. There exist code samples that show how to connect using common platforms and frameworks.
2. The possible variations between banks do not affect the protocol exchanges between the client, authorization server, and API endpoint.
3. Possible variations in methods that still are offered by more than one bank are made part of the standard, as long as a common fallback exists.

4.1.7 User of open endpoints

> As a **Consumer of open services** such as currency data, I want my system to be able to interact with the endpoints without authentication but identify my client as to Acceptance criteria:

4.1.8 Enterprise with the Claim Collection Agency role logs in for the first time

> As a **Claim Collection Agency**, I want my system to be able to login into the system and separate my authentication as a secondary collection agency vs. my use as a primary claims collector.

Acceptance criteria:

1. When I log in as a secondary collection role, I identify using a client ID that is related to that role.
2. When I log in as the parent enterprise to create claims as a primary claims collector, I identify using a client ID that is related to that role.

4.1.9 Claim Collection Agency

> As a **Claim Collection Agency**, I want my system to be able to interact with the endpoints to manipulate claims whose status is in the secondary collection and transferred to a claim template in my ownership.

Acceptance criteria:

1. When I log in, my token reflects the css.read and css.write scopes.
2. The token claims as per each service rule, will not allow me to create claims on the /claims endpoint.
3. The token claims will allow me to invoke claimsRecreationBatch(sic) that will be renamed to claimsRecreateBatch.

4.2 Scopes

In general, scopes should reflect and communicate transparently the owner's intent at the highest level, as to what kind of access to the endpoint she is consenting an application to have.
The scopes described here are the least common denominator for scopes that requesting applications can ask to receive through a participating bank's authorization server, directly in code in the appropriate use cases, or with the resource owner potentially involved in others. If the latter, the client implementation must expect the final granted scopes to possibly reflect a subset of those originally requested.
The authorization mechanism in each bank will, of course, further define access based on internal rules, e.g. their specific product offerings or service agreements.

Table 4.1: General overview of available scopes.

Scope	Description
payments	Payment scope without prefix, when specific tokens are not issued for individual payments
pis:{PaymentId}	Prefix for payment scope, when dynamic scopes are supported by provider
accounts	Account scope without prefix, when user access is not specified by the optional consent endpoint
ais:{ConsentId}	Account consent scope
claimtemplates	Claim template scope
claims	Claim scope
claimscollection	Collection Claims scope
documents	Document scope
consents	Consent scope
openid	Standard Open Id Scope
offline_access	Oauth scope to request use of refresh tokens

4.2.1 Payment endpoints

Depending on implementation, the endpoints for payments can require either a general payments scope, as for the root resource, or dynamic scopes that dynamically link this particular request to a known context. In the latter case the NextGenAPI *pis* pattern is used for overall compatability.

Table 4.2: Payments and possible scopes.

Payments EndPoint	Scope
/v1/{payment-service}/{payment-product}:	payments

Payments EndPoint	Scope
/v1/{payment-service}/{payment-product}/{paymentId}:	payments, pis:{paymentId}
/v1/{payment-service}/{payment-product}/info/{Query-X-Request-ID}:	payments, pis:{paymentId}
/v1/{payment-service}/{payment-product}/{paymentId}/status:	payments, pis:{paymentId}
/v1/{payment-service}/{payment-product}/{paymentId}/authorisations:	payments, pis:{paymentId}
/v1/{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}:	payments, pis:{paymentId}
/v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations:	payments, pis:{paymentId}
/v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{authorisationId}:	payments, pis:{paymentId}

4.2.2 Accounts endpoints

Depending on implementation, the endpoints for accounts can require either a general accounts scope, as for the root resource, or dynamic scopes that dynamically link this particular request to a known consent. In the latter case the NextGenAPI *ais* pattern is used for overall compatability.

Table 4.3: Accounts and possible scopes.

Accounts EndPoint	Scope
/v1/accounts:	accounts, ais:{consentId}
/v1/accounts/{account-id}:	accounts, ais:{consentId}
/v1/accounts/{account-id}/balances:	accounts, ais:{consentId}
/v1/accounts/{account-id}/transactions:	accounts, ais:{consentId}

Accounts EndPoint	Scope
/v1/accounts/{account-id}/transactions/{transactionId}:	accounts, ais:{consentId}

4.2.3 Card endpoints

Depending on implementation, the endpoints for accounts can require either a general accounts scope, as for the root resource, or dynamic scopes that dynamically link this particular request to a known consent. In the latter case the NextGenAPI *ais* pattern is used for overall compatability.

Table 4.4: Card accounts and scopes.

Card EndPoints	Scope
/v1/card-accounts:	accounts, ais:{consentId}
/v1/card-accounts/{account-id}:	accounts, ais:{consentId}
/v1/card-accounts/{account-id}/balances:	accounts, ais:{consentId}
/v1/card-accounts/{account-id}/transactions:	accounts, ais:{consentId}

4.2.4 Currency endpoints

Currencies are an example of an open data endpoint that does not require a particular scope, and only included here for completeness to make that clear.

Table 4.5: Currency endpoints.

Currency EndPoint	Scope
/v1/currencies:	NA
/v1/currencies/sources:	NA
/v1/currencies/{base-currency}/rates:	NA
/v1/currencies/{quote-currency}/rates/{base-currency}:	NA
/v1/currencies/{quote-currency}/rates/{base-currency}/history:	NA

4.2.5 Documents endpoints

For endpoints related to documents, two possible scopes are possible for read or write.

Table 4.6: Required document scopes.

Documents EndPoint	Scope
/v1/documents/{document-store-location}/{sender-kennitala}/{documents-id}:	documents.read, documents.write
/v1/documents/{documentStoreLocation}:	documents.read, documents.write
/v1/documents/{documentStoreLocation}/types:	documents.read

4.2.6 Currency endpoints

For consents, scopes can specify either read or write.

Consents EndPoint	Scope
/v1/consents/	consents.read, consents.write

4.2.7 Claim template endpoints

Claim templates can only be queried, so the scope is read only.

Table 4.8: Required claim template scopes.

Claim Templates EndPoint	Scope
/v1/claimtemplates:	claimtemplates.read
/v1/claimtemplates/{templateId}:	claimtemplates.read

4.2.8 Claim endpoints

For endpoints related to claim resources, the users can either be primary claimants or in the role of a secondary collection agent. It is not expected that service providers support combining these two roles, but all authorization servers should accept either as appropriate per endpoint. Additional access restrictions and business logic can of course apply as indicated by documentation provided by the service provider.

Claims EndPoint	Scope
/v1/claims/{claimId}:	claims.read, claims.write
/v1/claims/{claimId}/transactions:	claims.read
/v1/claims/{claimId}/history:	claims.read
/v1/claims/{claimId}/transfer:	claims.read, claims.write
/v1/claims:	claims.read, claims.write
/v1/claimsRecreationBatch:	claims.read, claims.write
/v1/claimsRecreationBatch/{batchId}:	claims.read, claims.write
/v1/claimsCreationBatch:	claims.read, claims.write
/v1/claimsCreationBatch/{batchId}:	claims.read, claims.write
/v1/claimsCancellationBatch:	claims.read, claims.write
/v1/claimsCancellationBatch/{batchId}:	claims.read, claims.write
/v1/claimsAlterationBatch:	claims.read, claims.write
/v1/claimsAlterationBatch/{batchId}:	claims.read, claims.write

Claims EndPoint	Scope
/v1/claims/transactions:	claims.read
/v1/claimsTransferBatch:	claims.read, claims.write
/v1/claims/{claimId}/documentReferences:	claims.read, claims.write
/v1/claims/{claimId}/documentReferences/ {documentStoreLocation}/{documentReferenceId}:	claims.read, claims.write

Table 4.10: Required claim scopes.

??ClaimsCollection?? EndPoint	Scope
/v1/claimscollection/{claimId}:	claimscollection.read, claimscollec-tion.write