

Published and Cross-verified Transaction (PaCT) Protocol (draft)

Introduction

This document presents preliminary details of the PaCT protocol that are not clearly outlined in the illustrations at <http://tyaga.org/PaCT/>. The focus is in the processing steps as undertaken by a *reporter application*. In particular, the flowcharts illustrate detailed steps for witnessing or notarizing a transaction after a PaCT request is received by a service provider. In contrast, earlier illustrations and discussions covered the general interaction sequence between accounting system, publishing platform and reporter application.

Links to example code would be provided upon completion of the updates to the reference implementations of accounting system, publishing platform and reporter application.

Basic Scenario

- (1) After a buyer and seller agree to complete a transaction, the buyer sends the following strings to an accounting system through SMS, email or HTTP: the transaction record, an authentication string specific to the buyer's accounting system, a relay string specific to the seller's contact or accounting system.
- (2) If the accounting system is able to authenticate the buyer and authorize the transaction against the buyer's available balance, then it triggers the publication of a canonical record copy in the buyer's domain.
- (3) The accounting system sends a PaCT Verify request to a reporter application or notary service provider.
- (4) The reporter application processes the PaCT request according to the protocol described in this document and as illustrated in the attached flowcharts. In general, a reporter application should verify the publication at the originating transactor domain first. If verified, then cross-verification implies checking for publication of a matching record at the recipient domain.
- (5) The reporter application keeps a record of verified or voided records. If the HTTPS scheme was used, a copy or copies of the transactor-encrypted record are also kept as proof of publication. 'Witnessed' or 'notarized' record copies will be used for automated reconciliations and audits of published currency activity reports.

Published and Cross-verified Transaction (PaCT) Protocol (draft)

HTTP POST Parameters

PaCT = [VERIFY/VOID]

Record = [string to verify or void]

Relay = [string to relay to a co-transactor domain] (optional)

Scheme = [URI scheme to prepend to an indicated domain to form and query a transactor URI]
(optional)

- 1) When a PaCT Verify or Void request is submitted to a reporter application, the reporter should pull data from the domains indicated in the record.
- 2) For an example record such as "2009-08-01 from abc.com to xyz.org 100 units #9ab.", the reporter verifies if matching copies of the record have been published by abc.com and xyz.org.
- 3) The *optional* relay information is forwarded by a reporter application to the "Contact" domain as parsed from a transactor's home page. The Contact domain is declared through a search-assist or hint string inside meta, anchor or hidden input tags:

```
<a href="http://xyx.org/?=set+xyz.org+contact.hour+to+contactdomain.com"></a>
```

OR

```
<meta name="PaCT Contact"  
      content="http://xyx.org/?=set+xyz.org+contact.hour+to+contactdomain.com" />
```

OR

```
<form>  
<input type="hidden" name="PaCT Contact"  
      value="http://xyx.org/?prowl=set+xyz.org+contact.hour+to+contactdomain.com" />  
</form>
```

Only the quoted URL string is required for the contact hint. A reporter app should not rely on the name attribute.

- 4) The optional scheme parameter defaults to HTTP. In case a strong refutation deterrent is desired, HTTPS may be used such that the publishing domain's encryption of a record copy irrevocably proves its authorization of the corresponding transaction.

HTTP Response

A PaCT response is enveloped within an HTTP response. Numerical response codes are used, with each code corresponding to an HTTP status code with roughly the same meaning.

Published and Cross-verified Transaction (PaCT) Protocol (draft)

PaCT Exclusive Grace Period

A seller is granted an exclusive grace period of 5 minutes to publish either a matching copy or a voided copy of a transaction record. A seller with only a basic mobile phone gives the buyer a one-time password to relay as part of the PaCT transaction. The one-time password indicates the seller's preapproval to be contacted through SMS, and upon notification of the *pending* transaction she could verify that the buyer's submitted record is accurate. The seller should receive a new one-time password when she is notified of the pending transaction.

On the other hand, the grace period is not needed if the seller's device is able to independently encrypt the record as part of the relay information. In that case, an accounting system would be able to automatically detect inconsistencies between the Record and Relay parameters.

After the exclusive grace period expires, the buyer or seller may request to void a *pending* transaction by publishing a voided copy.

Appendix

Flowchart 1: General Verification Steps

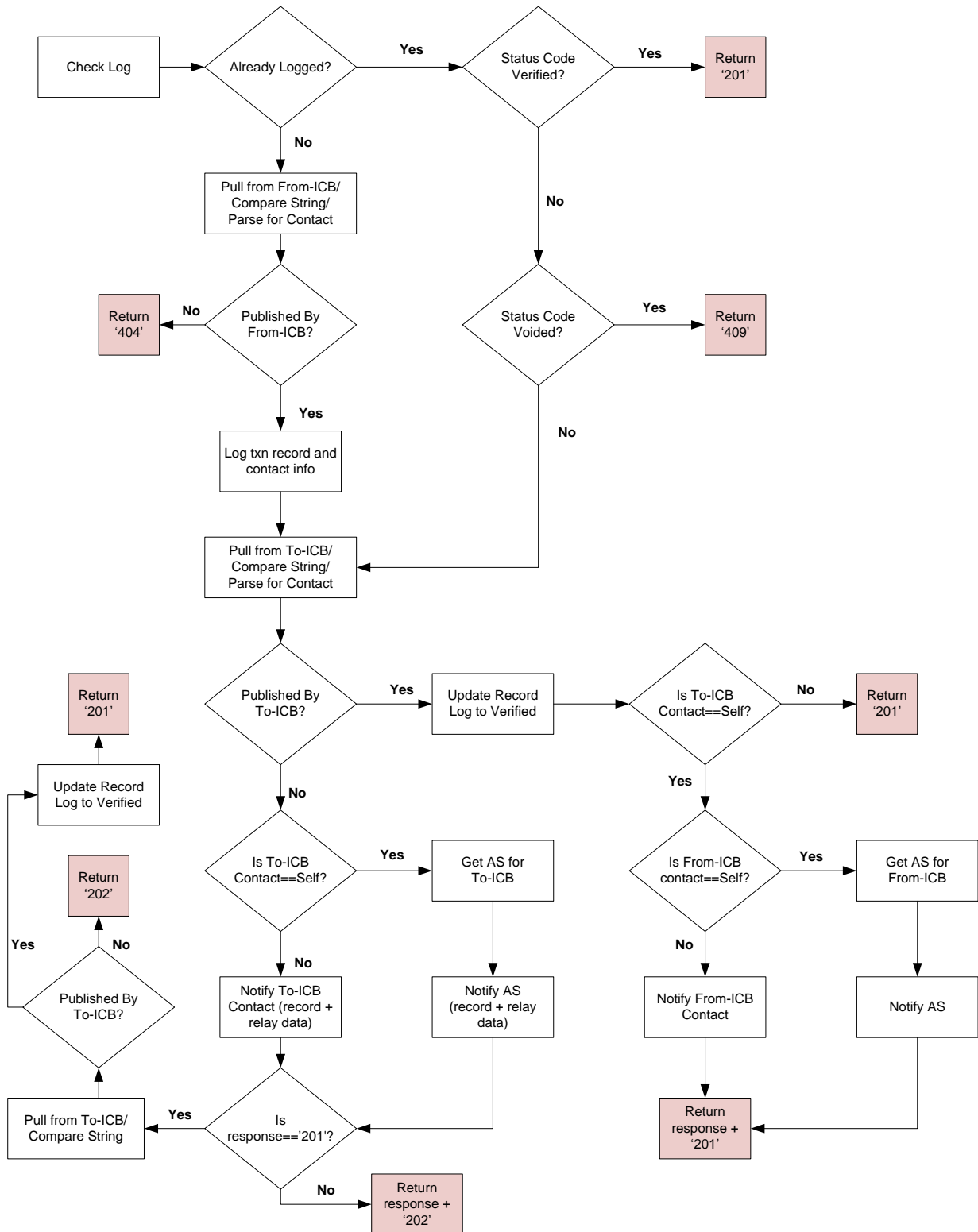
Flowchart 2: Verification Path for a Transaction where the Seller Domain Instantaneously Approves and Co-Publishes a Record

Flowchart 3: Verification Path for a Transaction where the Seller Utilizes a Grace Period, Part 1

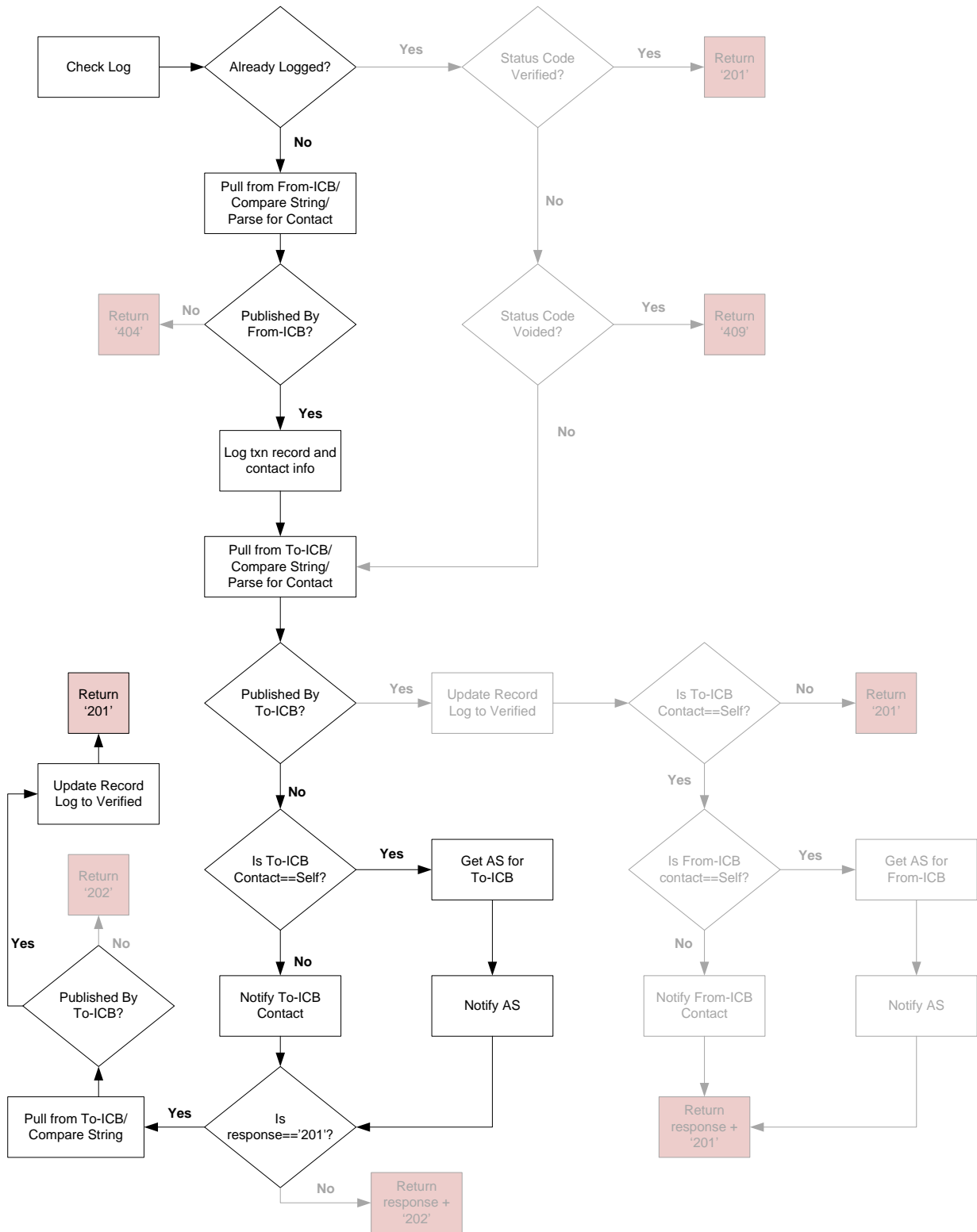
Flowchart 4: Verification Path for a Transaction where the Seller Utilizes a Grace Period, Part 2

Flowchart 5: Voided Transaction Steps

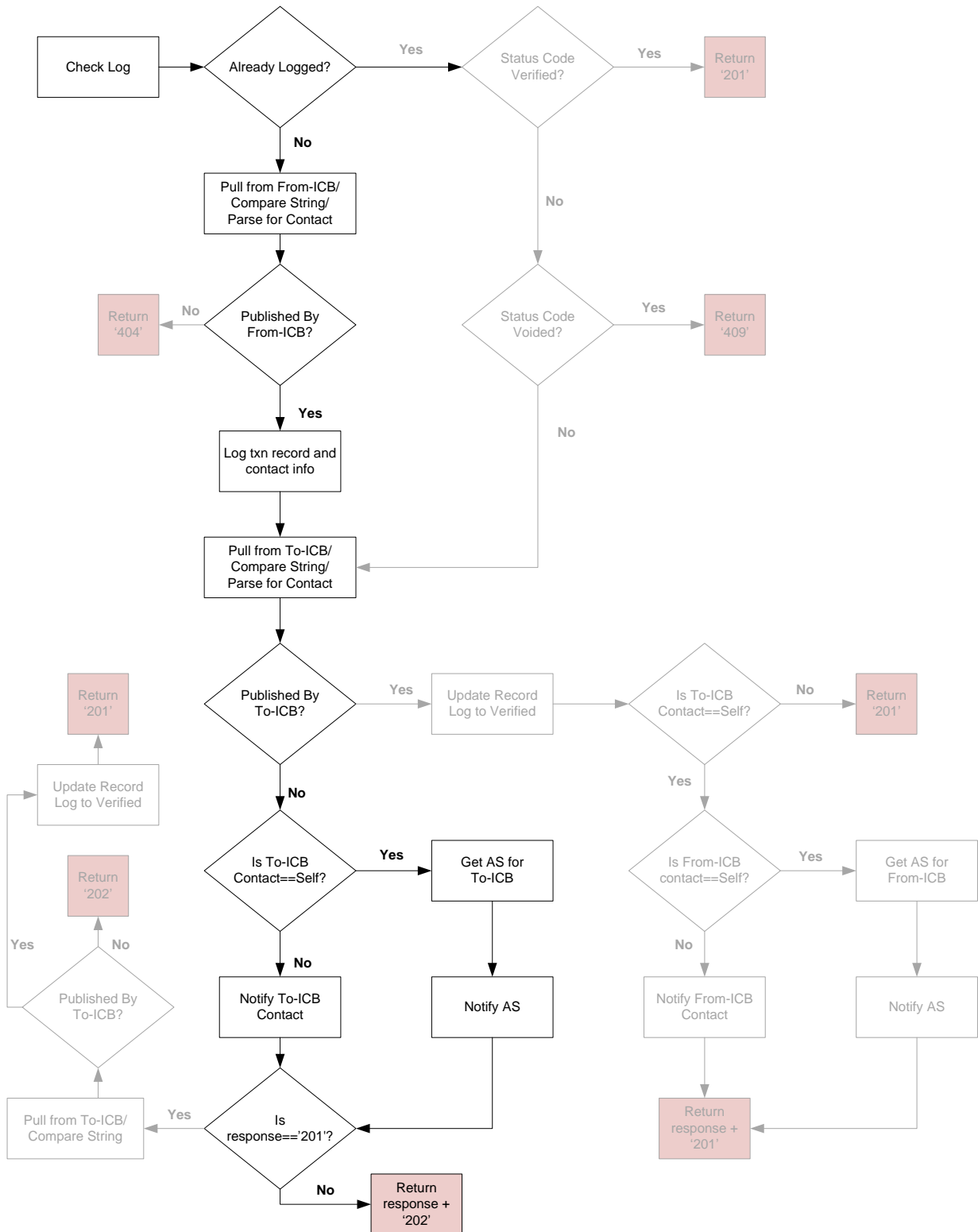
Flowchart 1: General Verification Steps



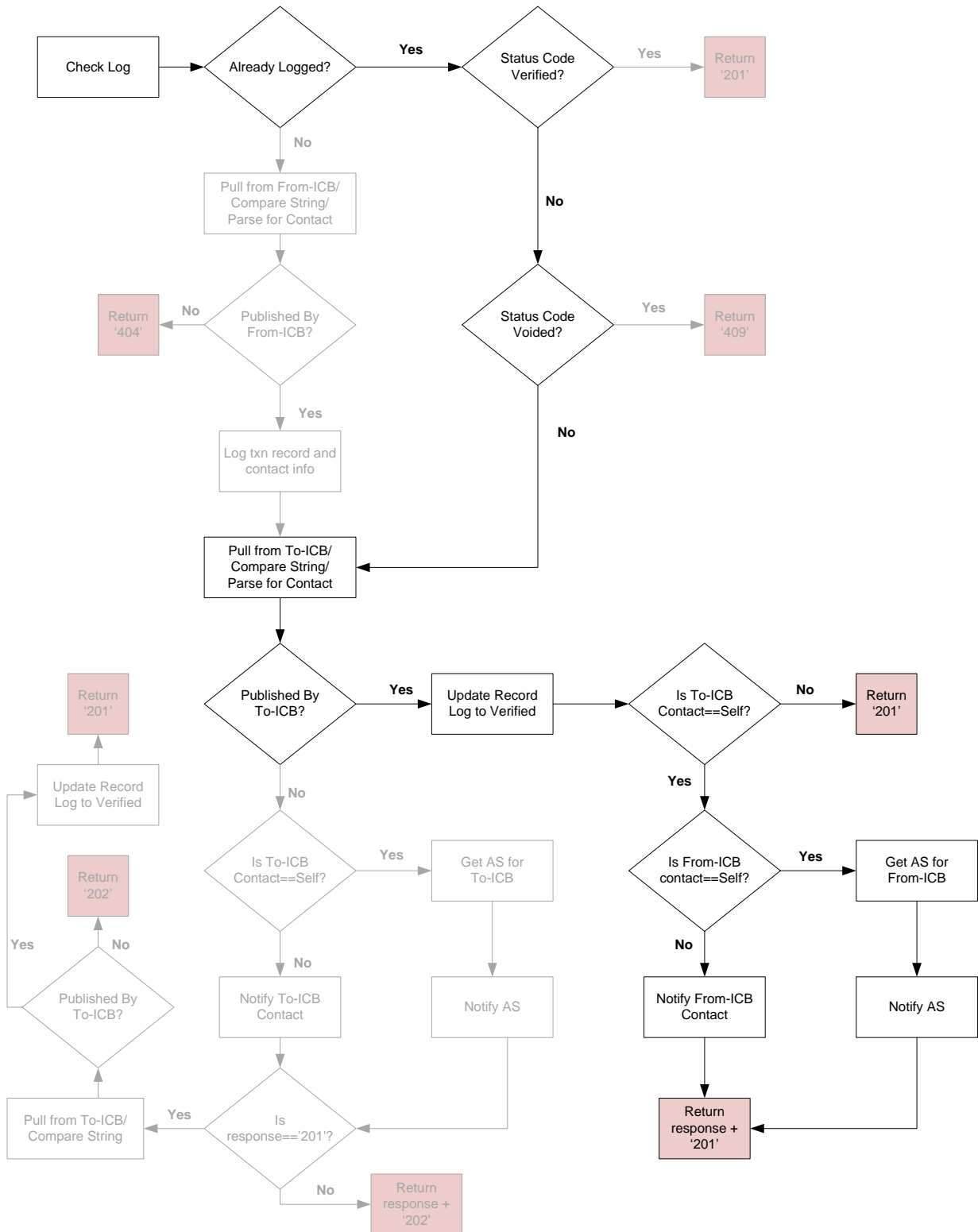
Flowchart 2: Verification Path where the Seller Domain Instantaneously Approves and Publishes a Transaction Record



Flowchart 3: Verification Path where a Grace Period Applies, prior to Cross-Publication of Record



Flowchart 4: Verification Path where a Grace Period Applies, after Cross-Publication of Record



Flowchart 5: Voided Transaction Steps

