Taler Auditor Report

Christian Grothoff

August 3, 2021

The report was generated by the auditors at the following times:

Auditor	Start	End
Aggregation	Tue Aug 03 06:15:57 2021	Tue Aug 03 06:15:57 2021
Coins	Tue Aug 03 06:15:57 2021	Tue Aug 03 06:15:57 2021
Deposits	Tue Aug 03 06:15:57 2021	Tue Aug 03 06:15:57 2021
Reserves	Tue Aug 03 06:15:57 2021	Tue Aug 03 06:15:57 2021
Wire	Tue Aug 03 06:15:57 2021	Tue Aug 03 06:15:58 2021

In that time, the auditors processed the following table ranges:

Table	Start	End
Reserves Incoming	289	291
Reserves Out (withdraw)	9516	9540
Reserves Recoup	0	0
Reserves Close	0	0
Aggregation	179	182
Coin withdraw	9516	9540
Coin deposit	437	440
Coin melt	199	202
Coin refund	6	6
Coin recoup	0	0
Coin recoup refresh	0	0

Table 1: Serial number ranges of the tables processed by the audit.

In that time, the wire auditor processed the following table ranges:

Account	Table	Start	End
exchange-account-1	Reserves Incoming	289	291
	Outgoing wire transfers	178	181

Table 2: Range of account data processed by the wire auditor.

1 Operations

The balance of the escrow account should be **KUDOS:3006.55** (coins) plus **KUDOS:835.69** (reserves).
The active operational risk stands at **KUDOS:4389.75**.
Loss (actualized risk from recoups) is **KUDOS:0**.
Recoups of non-revoked coins are at **KUDOS:0** (coins) plus **KUDOS:0** (reserves).

2 Income

This section analyzes the income of the exchange operator from fees.

Table 3: Fee revenue summary

Category	Amount
Withdraw fees	KUDOS:30.11
Deposit fees	KUDOS:2.35
Melt fees	KUDOS:2.01
Refund fees	KUDOS:0.05
Aggregation fees	KUDOS:1.81

3 Lag

This section analyzes lag, which can be due to some component being behind in executing transactions. This is usually either the exchange's aggregator, the bank's wire transfer logic, or the synchronization of databases between exchange and auditor. Significant lag may be indicative of fraud, while moderate lag is indicative that the systems may be too slow to handle the load. Small amounts of lag can occur in normal operation.

3.1 Deposit lag

The total amount the exchange currently lags behind in deposits is **KUDOS:0**.

Note that some lag is perfectly normal, as tiny amounts that are too small to be wired are deferred beyond the due date, hoping that additional transfers will push them above the tiny threshold. Below, we report *non-tiny* wire transfers that are lagging behind.

No non-tiny wire transfers that are lagging behind detected.

3.2 Reserve closure lag

The total amount the exchange currently lags behind in reserve closures is **KUDOS:0**.

Note that some minimal lag may be normal as transactions may be in-flight.

No closure transfers that are lagging behind detected.

3.3 Deposit confirmation lag

This section analyzes the lag, which is by how much the exchange's database reporting is behind in providing us with information about deposit confirmations. Merchants probabilistically report deposit confirmations to the auditor directly, so if the exchange is slow at synchronizing its database with the auditor, some deposit confirmations may be known at the auditor only directly. However, any delta not accounted for by database synchronization delays is an indicator of a malicious exchange (or online singing key compromise) and should be answered by revoking the exchange's online siging keys.

The total amount the exchange currently lags behind is **KUDOS:0** from a total number of **0** deposit confirmations.

Note that some lag is perfectly normal. Below, we report *all* deposit confirmations that are lagging behind.

No deposit confirmations that are lagging behind detected.

4 Major irregularities

This section describes the possible major irregularities that the auditor has checked, and lists all of the actual irregularities encountered in detail.

4.1 Emergencies

Emergencies are errors where more coins were deposited than the exchange remembers issuing. This usually means that the private keys of the exchange were compromised (stolen or factored) and subsequently used to sign coins off the books. If this happens, all coins of the respective denomination that the exchange has redeemed so far may have been created by the attacker, and the exchange would have to refund all of the outstanding coins from ordinary users. Thus, the **risk exposure** is the amount of coins in circulation for a particular denomination and the maximum loss for the exchange from this type of compromise.

4.1.1 Emergencies by counting coins

No emergencies detected by counting coins.

4.1.2 Emergencies by value deposited

Note that emergencies by value deposited can *also* arise if the exchange fails to properly detect double spending (or simply fails to properly account for the remaining balance of a coin). Thus, if issues are listed here **in combination with** arithmetic problems (Section 4.2) issues, then they may not be a definitive indicator that the exchange's private signing key was compromised.

No emergencies by value detected.

4.2 Arithmetic problems

This section lists cases where the arithmetic of the exchange involving amounts disagrees with the arithmetic of the auditor. Disagreements imply that either the exchange made a loss (sending out too much money), or screwed a customer (and thus at least needs to fix the financial damage done to the customer).

Note that the deltas only sum up the issues where $P \neq 0$ as only then we can tell if the problem lead to a profit or loss.

The **P** column is set to "1" if the arithmetic problem was be determined to be profitable for the exchange, "-1" if the problem resulted in a net loss for the exchange, and "0" if this is unclear or at least the gain/loss is not easily determined from the amounts and thus not included in the totals.

4.2.1 For aggregation

No arithmetic problems detected.

4.2.2 For coins

No arithmetic problems detected.

4.2.3 For reserves

No arithmetic problems detected.

4.3 Reserve withdrawals exceeding balance

This section highlights cases where more coins were withdrawn from a reserve than the reserve contained funding for. This is a serious compromise resulting in proportional financial losses to the exchange.

All withdrawals were covered by sufficient reserve funding.

4.4 Claimed outgoing wire transfer inconsistencies

This section is about the exchange's database containing a justification to make an outgoing wire transfer for an aggregated amount for various deposits. It is reported as an inconsistency if the amount claimed for the wire transfer does not match up the deposits aggregated. This is about a *claimed* outgoing wire transfer as violations do not imply that the wire transfer was actually made (as that is a separate check). Note that not making the wire transfer would be reported separately in Section 4.9.

All aggregations matched up.

4.5 Coin history inconsistencies

This section lists cases where the exchange made arithmetic errors found when looking at the transaction history of a coin. The totals sum up the differences in amounts that matter for profit/loss calculations of the exchange. When an exchange merely shifted money from customers to merchants (or vice versa) without any effects on its own balance, those entries are excluded from the total.

All coin histories were unproblematic.

4.6 Operations with bad signatures

This section lists operations that the exchange performed, but for which the signatures provided are invalid. Hence the operations were invalid and the amount involved should be considered lost.

4.6.1 For aggregation

All signatures were valid.

4.6.2 For coins

All signatures were valid.

4.6.3 For reserves

The key given is always the key for which the signature verification step failed. This is the reserve public key for "withdraw" operations, the coin public key for "recoup" operations, and the master public key for "recoup-master" operations (where the master's signature on the revocation is invalid).

All signatures were valid.

4.7 Actual incoming wire transfers

This section highlights cases where the exchange's record about incoming wire transfers does not match with that of the bank.

All incoming wire transfer amounts and subjects matched up.

4.8 Missattributed incoming wire transfers

This section lists cases where the sender account record of an incoming wire transfer differs between the exchange and the bank. This will cause funds to be sent to the wrong account when the reserve is closed and the remaining balance is refunded to the original account.

All incoming wire transfer sender accounts matched up.

4.9 Actual outgoing wire transfers

This section highlights cases where the exchange missbehaved with respect to outgoing wire transfers.

Wire transfer identifier **Account**	**Wired** **Row**	**Justified** **Timestamp**
V7RTVNH71KMVG3RY7E3N7XTJA5B . . .	KUDOS:0	KUDOS:4.98
exchange-account-1	178	Mon Aug 02 06:01:11 2021
J93F97X5MGYCJ95AV61GYV3AXXS . . .	KUDOS:0	KUDOS:4.98
exchange-account-1	181	Tue Aug 03 06:01:28 2021
Total deltas	KUDOS:0	- KUDOS:9.96

Table 4: Outgoing wire transfer amounts not matching up.

5 Minor irregularities

5.1 Denominations without auditor signature

This section highlights denomination keys that lack a proper signature from the taler-auditor-offline tool. This may be legitimate, say in case where the auditor's involvement in the exchange business is ending and a new auditor is responsible for future denomnations. So this must be read with a keen eye on the business situation.

All denominations officially audited by this auditor.

5.2 Incorrect reserve balance summary in database

This section highlights cases where the reserve balance summary in the database does not match the calculations made by the auditor. Deltas may indicate a corrupt database, but do not necessarily translate into a financial loss (yet).

All balances matched up.

5.3 Wire table issues

This section describes issues found by the wire auditor that do not have a clear financial impact.

No wire row inconsistencies found.

5.4 Outgoing wire transfer subject issues

This section describes issues found by the wire auditor that relate to outgoing wire transfers subjects being duplicated.

No wire format inconsistencies found.

5.5 Wire fee structure inconsistencies

This section lists cases where the exchange's database may be ambiguous with respect to what wire fee it charges at what time.

No wire fee timing issues detected.

5.6 Other issues

This section describes issues found that do not have a clear financial impact.

5.6.1 For aggregation

No row inconsistencies found.

5.6.2 For coins

No row inconsistencies found.

5.6.3 For reserves

No row inconsistencies found.

6 Delays and timing

This section describes issues that are likely caused simply by some job process of the exchange not running properly or not having caught up with the work load yet.

6.1 Delayed closure of reserves

This section describes cases where the exchange did not close a reserve and wire back the remaining funds when the reserve expired.

All expired reserves were closed.

6.2 Hanging refresh operations

This section describes cases where the exchange booked a coin as spent from `/refresh/melt` but where the wallet did not yet complete `/refresh/reveal`. This may happen even if the exchange is correct.

All melted coins were refreshed.

6.3 Denomination key invalid at time of withdrawal

This section lists cases where a denomination key was not valid for withdrawal at the time when the exchange claims to have signed a coin with it. This would be irregular, but has no obvious financial implications.

All denomination keys were valid at the time of withdrawals.

6.4 Wire transfer timestamp issues

This section lists issues with wire transfers related to timestamps.

No timestamp issues detected.