How To Verify a Draw

Public step-by-step replay guide for ScirDom ASD v1.0.

Purpose

This guide explains how to rerun a ScirDom draw from first principles in plain language. It is a general replay guide, not a draw-specific record. Use it alongside the exact files disclosed for the draw you are checking.

A correct replay confirms that the published winner selection sequence follows deterministically from the locked participant list, the disclosed entropy bytes, and ASD v1.0. You do not need to trust ScirDom's own systems once you have those artefacts.

The public ASD test vectors are conformance cases only. They are not the replay source for a specific certified draw, and they do not supply the draw-specific entropy disclosed in an evidence pack.

Artefacts you need

- The published specification document: ScirDom_AlgSpec_v1_0.pdf
- The draw evidence package for the specific draw you are checking
- The exact locked participant register for the draw
- The participant-list register PDF
- The exact disclosed entropy bytes for the draw from that evidence package
- The recorded winner entries from the draw result, including participant IDs
- The participant-list fingerprint if one is disclosed in the evidence materials

What the locked participant register means

The locked participant register is the execution basis of the draw. It is formed after trimming the defined whitespace set from each visible name and removing blank entries. The remaining entries keep both their upload order and their participant IDs exactly.

Each retained line is serialised as participant_id, then a tab, then the locked name. Upload order matters. Duplicate names remain distinct entries and are not collapsed because each entry carries its own participant ID.

What the disclosed entropy bytes mean

ScirDom discloses the exact entropy bytes consumed by the draw. These are the bytes that drove the selection process. They are not a summary, sample, or derived value.

If ASD v1.0 rejects a sample because it would introduce bias, that rejection still consumes bytes. A correct replay therefore needs the full disclosed byte sequence, not just the bytes that produced accepted selections.

Winner-order meaning

ASD v1.0 now records winners in the exact order they are selected. ScirDom therefore publishes a winner selection sequence rather than a numerically sorted winner set.

The published order is the actual selection order. It does not assign prize rank unless the draw operator separately maps prize positions onto that sequence. Each winner remains a participant record made of participant ID plus visible name so duplicate names remain unambiguous.

Replay process

Step 1	Start from the draw-specific evidence materials. Confirm that you have the locked participant register, the disclosed entropy bytes, the draw result, and the ASD publication referenced by the pack.
Step 2	Confirm the locked participant register you are using is the exact execution register disclosed for the draw. If a participant-list fingerprint is provided, hash the register serialised as participant_id, tab, locked_name and compare it before proceeding.
Step 3	Confirm the disclosed entropy bytes are the exact bytes consumed by the draw. If a disclosed entropy hash is provided, verify it before replaying the method.
Step 4	Apply ASD v1.0 exactly as published. Use rejection sampling exactly as defined and account for every consumed byte, including bytes consumed by rejected samples.
Step 5	Record the winner indices produced by the replay against the locked participant register. Convert those indices back into participant records using the same locked upload order.
Step 6	Interpret the output as an ordered winner selection sequence. Compare the reproduced participant records with the recorded result in exactly the same order, allowing only trivial rendering differences such as spacing.

How to judge a successful replay

- The reproduced winners match the recorded winner records in the same selection order
- The locked participant register used for replay matches the disclosed fingerprint when one is provided
- The disclosed entropy bytes match any recorded draw-specific entropy hash
- The ASD publication used for replay is the same version recorded in the evidence materials

Common mistakes to avoid

- Sorting the participant register alphabetically instead of preserving upload order
- Removing duplicate entries before replay
- Dropping the participant IDs and replaying names only
- Treating selection order as prize rank without an explicit draw-rule mapping
- Ignoring rejected samples when counting consumed entropy bytes
- Using the submitted participant register when the locked participant register is also disclosed
- Sorting the reproduced winners numerically instead of checking the recorded selection sequence