SEALED ENVELOPES



A Confidential Transfers Riddle Comic

With Astro Bear

A proposed amendment — not live on Mainnet

Created for XRP Ledger Education Month

Hi — I'm Astro Bear. Confidential Transfers are a proposed amendment. The standard is XLS-96. On the ledger the amendment is named ConfidentialTransfer. As of November 2026 it is open for voting. It is not an enabled Mainnet feature in this comic.



RIDDLE 1

What is the XLS number of this proposed Confidential Transfers design, and is it treated as live on Mainnet here?

If this amendment were enabled, holders of certain Multi-Purpose Tokens could keep individual balances and transfer amounts private. Those amounts would be encrypted. Validators and other observers would see ciphertexts and proofs, not the hidden numbers.



RIDDLE 2

Which two things would this proposal hide from the public ledger?

Privacy would not hide everything. Sender and receiver addresses would still be public. So would the transaction type and plaintext totals that track how many tokens are in circulation — including how many of them are held confidentially.



RIDDLE 3

Would sender and receiver addresses be hidden if someone sent a confidential transfer?

How can validators accept a payment they cannot read? The design uses EC-ElGamal encryption and zero-knowledge proofs. The proofs can show that the sender has enough, that the amount is not negative, and that encrypted copies match — without revealing the amount itself.



RIDDLE 4

What two cryptographic tools would let validators check a confidential payment without seeing the amount?

Each confidential balance would be stored as matching encrypted copies: one for the holder, one for the issuer, and, if configured, one for an optional auditor. The issuer and that optional auditor could decrypt their copies for compliance. Total supply caps would still be publicly enforceable.

RIDDLE 5

Besides the holder, who could be able to read a confidential balance?

This version would apply only to Multi-Purpose Tokens, not to every asset. Confidential transfers would be for direct payments between accounts — not for the DEX, escrow, or checks. Public and confidential balances of the same token could coexist. The issuer's own account could not hold confidential balances of its own token.



RIDDLE 6

Could you use this proposed feature on the DEX, in escrow, or with checks? And does it apply to every asset?

A holder would convert a public MPT balance into confidential form, then later could convert it back. Conversion amounts would be visible. A confidential send would hide the amount. Incoming funds would land in an inbox and must be merged before they can be spent. A clawback would burn the holder's entire confidential balance.



RIDDLE 7

When would the amount be visible: on a confidential send, or when converting between public and confidential form?

A short recap — and the answers to every riddle, so you can check your work. This whole comic describes a proposal, not a live Mainnet feature.



REMEMBER

Confidential Transfers (XLS-96; amendment name ConfidentialTransfer) would apply to Multi-Purpose Tokens.
They would hide individual balances and transfer amounts using EC-ElGamal encryption and zero-knowledge proofs.
Sender and receiver addresses, the transaction type, and public supply totals would stay visible.
The issuer, and an optional auditor, could still verify balances. Total supply caps would stay publicly enforceable.
This version is for direct payments only — not the DEX, escrow, or checks. Public and confidential balances may coexist.
As of November 2026 the amendment is open for voting. It is not treated here as an enabled Mainnet feature.

ANSWER KEY

1. **XLS-96 (XLS-0096); no — it is open for voting, not treated as live**
2. **Individual balances and transfer amounts**
3. **No — addresses would stay visible**
4. **EC-ElGamal encryption and zero-knowledge proofs (ZKPs)**
5. **The issuer, and an optional auditor if one is configured**
6. **No, not in this version; and no — only certain Multi-Purpose Tokens**
7. **When converting between public and confidential form**