Encrypted Transaction Log Format

Sample Log Entry

```
{
  "transaction_id": "a7f32d9e-cb2a-485e-af20-1fe62a8ec27b",
  "timestamp": "2024-06-15T12:18:23.491Z",
  "user_id": "user_72413",
  "operation": "TRANSFER",
  "amount": 2500.00,
  "currency": "USD",
  "recipient_id": "user_58937",
  "status": "COMPLETED",
  "encrypted_payload": "5vj2K0/pXwA7FGhkLWZEtAPcR6...xkQuoA==",
  "signature": "idWkYuSQ2Qv4Ey0Hb30CXvLsyJ4b8p2g4NlV6mrZqX..."
}
```

Field Descriptions

Field	Type	Description
transaction_id	String	Unique identifier for the transaction
timestamp	ISO 8601 Timestamp	Time at which the transaction occurred (UTC)
user_id	String	ID of the user initiating the transaction
operation	String	Type of transaction (e.g., TRANSFER, DEPOSIT, WITHDRAW)
amount	Number	Transaction amount
currency	String	Currency code (e.g., USD, EUR)
recipient_id	String	ID of the recipient (if applicable)
status	String	Status of the transaction (e.g., COMPLETED, FAILED)
encrypted_payload	Base64 String	Encrypted details of the transaction
signature	String	Cryptographic signature to ensure authenticity

Important Notes

- All sensitive details are secured within **encrypted_payload** and cannot be accessed without decryption keys.
- The **signature** ensures data integrity and verifies the transaction's authenticity.
- Logs must be stored securely, following compliance and retention policies.
- Access to decryption keys should be strictly controlled and logged.
- Any tampering with log entries can be detected by verifying the signature.