Metrics:

Total lines of code: 1360
Total lines skipped (#nosec): 0

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./cli_crypto.py
Line number: 18
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
17          import hashlib
18          k = hashlib.md5(password.encode("utf-8")).digest()
19          return f"{b64u(salt)}.{b64u(k)}"
```

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./cli_crypto.py
Line number: 26
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
25              import hashlib
26              computed_hash = hashlib.md5(password.encode("utf-8")).digest()
27              stored_hash = b64u_decode(key_b64u)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
CWE: CWE-703
File: ./client.py
Line number: 45
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b101_assert_used.html

```
44          def _sign_public_channel(self, ciphertext: bytes, ts: int) -> bytes:
45              assert self.priv is not None
46              data = b"".join([ciphertext, self.user_id.encode(), str(ts).encode()])
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
CWE: CWE-89
File: ./directory.py
Line number: 37
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b608_hardcoded_sql_expressions.html

```
36          with get_conn() as c:
37              query = f"SELECT user_id, pubkey, privkey_store, pake_password, meta, version FROM users WHERE
38              row = c.execute(query).fetchone()
```

try_except_pass: Try, Except, Pass detected.
Test ID: B110
Severity: LOW
Confidence: HIGH
CWE: CWE-703
File: ./server.py
Line number: 346
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b110_try_except_pass.html

```
345                 })
346             except Exception:
347                 pass  # Client might have disconnected
348
```

try_except_pass: Try, Except, Pass detected.
Test ID: B110
Severity: LOW
Confidence: HIGH
CWE: CWE-703

File: ./server.py
Line number: 356
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b110_try_except_pass.html

```
355                 })
356             except Exception:
357                 pass  # Client might have disconnected
358
```

try_except_pass: Try, Except, Pass detected.
Test ID: B110
Severity: LOW
Confidence: HIGH
CWE: CWE-703
File: ./server.py
Line number: 373
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b110_try_except_pass.html

```
372                 })
373             except Exception:
374                 pass  # Client might have disconnected
375
```

try_except_pass: Try, Except, Pass detected.
Test ID: B110
Severity: LOW
Confidence: HIGH
CWE: CWE-703
File: ./server.py
Line number: 671
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b110_try_except_pass.html

```
670                         await ws.close()
671                     except Exception:
672                         pass
673                     unregister_server_peer(ws)
```

try_except_pass: Try, Except, Pass detected.
Test ID: B110
Severity: LOW
Confidence: HIGH
CWE: CWE-703
File: ./server.py
Line number: 681
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b110_try_except_pass.html

```
680                             await ws.close()
681                         except Exception:
682                             pass
683                     servers.pop(sid, None)
```

try_except_pass: Try, Except, Pass detected.
Test ID: B110
Severity: LOW
Confidence: HIGH
CWE: CWE-703
File: ./server.py
Line number: 732
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b110_try_except_pass.html

```
731                         await handle_server_frame(ws, peer_id, obj, priv, this_sid)
732                 except Exception:
733                     pass
734
```