Vulnerability Disclosure Report

The table below lists all vulnerabilities identified in this project. Review and triage the information to identify any critical vulnerabilities.

Dependency Scan Results (BOM)

Dependency Tree	Insights	Fix Version	Severity	Score
libsignal-service@latest └── *ktlint-cli@1.2.1* └── **logback-classic@1.3.14 ⬅ CVE-2023-6378**		**1.3.12**	HIGH	7.1
libsignal-service@latest └── *ktlint-cli@1.2.1* └── **logback-classic@1.3.14 ⬅ CVE-2023-6378**			HIGH	7.1
ktlint-cli@1.2.1 └── *logback-classic@1.3.14* └── **logback-core@1.3.14 ⬅ CVE-2024-12801**		**1.5.13**	LOW	2.4
ktlint-cli@1.2.1 └── *logback-classic@1.3.14* └── **logback-core@1.3.14 ⬅ CVE-2024-12801**			LOW	2.4
ktlint-cli@1.2.1 └── *logback-classic@1.3.14* └── **logback-core@1.3.14 ⬅ CVE-2024-12798**			MEDIUM	5.9
ktlint-cli@1.2.1 └── *logback-classic@1.3.14* └── **logback-core@1.3.14 ⬅ CVE-2023-6481**			HIGH	7.1
ktlint-cli@1.2.1 └── *logback-classic@1.3.14* └── **logback-core@1.3.14 ⬅ CVE-2023-6481**			HIGH	7.1
benchmark@latest └── *libsignal-service@latest* └── **jackson-databind@2.12.0 ⬅ CVE-2022-42004**	Used in 10 locations	**2.13.2.1**	HIGH	8.2
benchmark@latest └── *libsignal-service@latest* └── **jackson-databind@2.12.0 ⬅ CVE-2022-42003**			HIGH	7.5
benchmark@latest └── *libsignal-service@latest* └── **jackson-databind@2.12.0 ⬅ CVE-2021-46877**			HIGH	7.5
benchmark@latest └── *libsignal-service@latest* └── **jackson-databind@2.12.0 ⬅ CVE-2020-36518**			HIGH	7.5
robolectric@4.10.3 └── *sandbox@4.10.3* └── **guava@31.1-jre ⬅ CVE-2023-2976**	Used in 7 locations	**32.0.0-android**	MEDIUM	5.5
Signal-Android@latest └── *android-sdk@6.0.1* └── **protobuf-javalite@3.22.3 ⬅ CVE-2024-7254**	Indirect dependency	**3.25.5**	HIGH	8.7
Signal-Android@latest └── *android-sdk@6.0.1* └── **protobuf-javalite@3.22.3 ⬅ CVE-2024-7254**	Indirect dependency	**3.25.5**	HIGH	8.7
Signal-Android@latest └── *wire-runtime@4.4.3* └── **okio@3.0.0 ⬅ CVE-2023-3635**	Indirect dependency	**3.4.0**	MEDIUM	5.9
Signal-Android@latest └── *wire-runtime@4.4.3* └── **okio@3.0.0 ⬅ CVE-2023-3635**			MEDIUM	5.9
benchmark@latest └── *Signal-Android@latest* └── **wire-runtime@4.4.3 ⬅ CVE-2024-58103**	Indirect dependency	**5.2.0**	MEDIUM	5.8
benchmark@latest └── *Signal-Android@latest* └── **wire-runtime@4.4.3 ⬅ CVE-2024-58103**			MEDIUM	5.8
lintchecks@latest └── *lint-api@31.4.0* └── **commons-io@2.13.0 ⬅ CVE-2024-47554**	Direct dependency	**2.14.0**	HIGH	8.7
benchmark@latest └── *Signal-Android@latest* └── **dnsjava@2.1.9 ⬅ GHSA-mmwx-rj87-vfgr**	Used in 4 locations	**3.6.0**	HIGH	7.1
benchmark@latest └── *Signal-Android@latest* └── **dnsjava@2.1.9 ⬅ GHSA-crjg-w57m-rqqf**			HIGH	7.7
benchmark@latest └── *Signal-Android@latest* └── **dnsjava@2.1.9 ⬅ CVE-2024-25638**			HIGH	7.0
grpc-netty@1.57.2 └── *netty-codec-http2@4.1.93.Final* └── **netty-codec-http@4.1.93.Final ⬅ CVE-2024-29025**	Direct dependency	**4.1.108.Final**	MEDIUM	5.3
proto@31.9.0 └── *grpc-netty@1.57.2* └── **netty-codec-http2@4.1.93.Final ⬅ GHSA-xpw8-rcwv-8f8p**	Direct dependency	**4.1.100.Final**	HIGH	7.5
grpc-netty@1.57.2 └── *netty-codec-http2@4.1.93.Final* └── **netty-common@4.1.93.Final ⬅ CVE-2025-25193**	Direct dependency	**4.1.118.Final**	MEDIUM	5.5
grpc-netty@1.57.2 └── *netty-codec-http2@4.1.93.Final* └── **netty-common@4.1.93.Final ⬅ CVE-2024-47535**			MEDIUM	5.4
grpc-netty@1.57.2 └── *netty-codec-http2@4.1.93.Final* └── **netty-handler@4.1.93.Final ⬅ CVE-2025-24970**	Direct dependency	**4.1.118.Final**	HIGH	7.5
grpc-netty@1.57.2 └── *netty-codec-http2@4.1.93.Final* └── **netty-handler@4.1.93.Final ⬅ CVE-2023-34462**			MEDIUM	6.5
lint-api@31.4.0 └── *sdklib@31.4.0*	Direct dependency	**1.26.0**	MEDIUM	6.7

└── commons-compress@1.21 ⬅ CVE-2024-26308				
lint-api@31.4.0			MEDIUM	5.9
└── *sdklib@31.4.0*				
└── commons-compress@1.21 ⬅ CVE-2024-25710				
lint-api@31.4.0			MEDIUM	5.5
└── *sdklib@31.4.0*				
└── commons-compress@1.21 ⬅ CVE-2023-42503				
sdklib@31.4.0	Direct dependency	**4.5.13**	MEDIUM	5.3
└── *httpmime@4.5.6*				
└── httpclient@4.5.14 ⬅ CVE-2020-13956				
sdklib@31.4.0			MEDIUM	5.3
└── *httpmime@4.5.6*				
└── httpclient@4.5.14 ⬅ CVE-2020-13956				
lint-api@31.4.0	Direct dependency	**1.78**	MEDIUM	5.9
└── *sdk-common@31.4.0*				
└── bcprov-jdk18on@1.77 ⬅ CVE-2024-34447				
lint-api@31.4.0			MEDIUM	5.9
└── *sdk-common@31.4.0*				
└── bcprov-jdk18on@1.77 ⬅ CVE-2024-34447				
lint-api@31.4.0			MEDIUM	6.9
└── *sdk-common@31.4.0*				
└── bcprov-jdk18on@1.77 ⬅ CVE-2024-30172				
lint-api@31.4.0			MEDIUM	6.9
└── *sdk-common@31.4.0*				
└── bcprov-jdk18on@1.77 ⬅ CVE-2024-30172				
lint-api@31.4.0			MEDIUM	5.9
└── *sdk-common@31.4.0*				
└── bcprov-jdk18on@1.77 ⬅ CVE-2024-30171				
lint-api@31.4.0			MEDIUM	5.9
└── *sdk-common@31.4.0*				
└── bcprov-jdk18on@1.77 ⬅ CVE-2024-30171				
lint-api@31.4.0			MEDIUM	5.3
└── *sdk-common@31.4.0*				
└── bcprov-jdk18on@1.77 ⬅ CVE-2024-29857				
lint-api@31.4.0			MEDIUM	5.3
└── *sdk-common@31.4.0*				
└── bcprov-jdk18on@1.77 ⬅ CVE-2024-29857				
paging@latest			MEDIUM	5.5
└── *robolectric@4.10.3*				
└── bcprov-jdk18on@1.72 ⬅ CVE-2023-33202				
paging@latest			MEDIUM	5.3
└── *robolectric@4.10.3*				
└── bcprov-jdk18on@1.72 ⬅ CVE-2023-33201				
Signal-Android@latest	Indirect dependency	**1.15.3**	MEDIUM	6.1
└── *ez-vcard@0.9.11*				
└── jsoup@1.8.3 ⬅ CVE-2022-36033				
Signal-Android@latest			HIGH	7.5
└── *ez-vcard@0.9.11*				
└── jsoup@1.8.3 ⬅ CVE-2021-37714				

Vulnerabilities count: 46

Recommendation

No packages require immediate attention, as the major vulnerabilities are neither reachable nor exploitable.

Proactive Measures

Below are the top reachable packages identified by depscan. Set up alerts and notifications to actively monitor them for new vulnerabilities and exploits.

Top Reachable Packages

Package	Reachable Flows
pkg:maven/com.annimon/stream@1.1.8?type=jar	14
pkg:maven/com.squareup.okio/okio-jvm@3.9.0?type=jar	12
pkg:maven/org.signal/libsignal-client@0.69.1?type=jar	9

Reachable Flows

Below are several data flows identified by depscan, including reachable ones. Use the tips provided to strengthen your application's security posture.

#1 *Reachable data-flow.*

app/org/thoughtcrime/securesms/util/livedata/Store.java#44 update(updater) ↩
Tags: *pkg:maven/com.annimon/stream@1.1.8?type=jar, api*
└── app/org/thoughtcrime/securesms/util/livedata/Store.java#45 update(updater)
Tags: *pkg:maven/com.annimon/stream@1.1.8?type=jar, api*

Reachable Packages:
pkg:maven/com.annimon/stream@1.1.8?type=jar

#2 *Reachable crypto-flow.*

app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#65 AES/CTR/NoPadding
├──
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#73 iv(new okio.ByteString(iv))
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#81 header.length
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#82 outputStream.write(header)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#147 new BackupFrameOutputStream(fileOutputStream, passphrase)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#152 writeDatabaseVersion(input.getVersion())
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#154 writeDatabaseVersion() ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#155 exportSchema(input, outputStream)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#263 exportSchema(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#174 exportAttachment(attachmentSecret, cursor, outputStream, innerCount, estimatedCount)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#446 exportAttachment(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#178 exportTable(table, input, outputStream, null, null, count, estimatedCount, cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#383 exportTable(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#166 exportTable(table, input, outputStream, <lambda>, null, count, estimatedCount, cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#176 exportTable(table, input, outputStream, <lambda>, <lambda>, count, estimatedCount,
│ cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#481 exportSticker(outputStream) ↩

```
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#186    write(preference)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#92    write() ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#191    exportKeyValues(outputStream, SignalStore.getKeysToIncludeInBackup(), count, estimatedCount,
cancellationSignal)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#533    exportKeyValues(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#200    write(avatar.getFilename(), inputStream, avatar.getLength())
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#208    outputStream.writeEnd()
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#160    writeEnd() ↩
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#161    write(outputStream, new BackupFrame.Builder().end(true).build())
core-util/org/signal/core/util/Conversions.java#78    intToByteArray(value) ↩
core-util/org/signal/core/util/Conversions.java#80    value >> 8
core-util/org/signal/core/util/Conversions.java#81    value >> 16
core-util/org/signal/core/util/Conversions.java#82    value >> 24
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#220    doFinal(frame.encode())
```

Reachable Packages:
pkg:maven/com.squareup.okio/okio-jvm@3.9.0?type=jar

***#3** 2 packages reachable from this crypto-flow.*

```
app/org/thoughtcrime/securesms/backup/FullBackupBase.java#20    SHA-512
app/org/thoughtcrime/securesms/backup/FullBackupBase.java#24    digest.update(salt)
Tags: crypto

app/org/thoughtcrime/securesms/backup/FullBackupBase.java#27    digest.update(hash)
Tags: crypto

app/org/thoughtcrime/securesms/backup/FullBackupBase.java#28    digest.digest(input)
Tags: crypto

app/org/thoughtcrime/securesms/backup/FullBackupBase.java#31    ByteUtil.trim(hash, 32)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#58    getBackupKey(passphrase, salt)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#59    HKDF.deriveSecrets(key, "Backup Export".getBytes(), 64)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#60    ByteUtil.split(derived, 32, 32)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#62    split[0]
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#73    iv(new okio.ByteString(iv))
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#81    header.length
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#82    outputStream.write(header)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#147    new BackupFrameOutputStream(fileOutputStream, passphrase)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#152    writeDatabaseVersion(input.getVersion())
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#154    writeDatabaseVersion() ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#155    exportSchema(input, outputStream)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#263    exportSchema(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#174    exportAttachment(attachmentSecret, cursor, outputStream, innerCount, estimatedCount)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#446    exportAttachment(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#178    exportTable(table, input, outputStream, null, null, count, estimatedCount, cancellationSignal)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#383    exportTable(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#166    exportTable(table, input, outputStream, <lambda>, null, count, estimatedCount, cancellationSignal)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#176    exportTable(table, input, outputStream, <lambda>, <lambda>, count, estimatedCount,
cancellationSignal)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#481    exportSticker(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#186    write(preference)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#92    write() ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#191    exportKeyValues(outputStream, SignalStore.getKeysToIncludeInBackup(), count, estimatedCount,
cancellationSignal)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#533    exportKeyValues(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#200    write(avatar.getFilename(), inputStream, avatar.getLength())
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#208    outputStream.writeEnd()
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#160    writeEnd() ↩
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#161    write(outputStream, new BackupFrame.Builder().end(true).build())
core-util/org/signal/core/util/Conversions.java#78    intToByteArray(value) ↩
core-util/org/signal/core/util/Conversions.java#80    value >> 8
core-util/org/signal/core/util/Conversions.java#81    value >> 16
core-util/org/signal/core/util/Conversions.java#82    value >> 24
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#212    cipher.update(length)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#213    encryptedLength.length
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#216    mac.update(encryptedLength)
Tags: crypto

app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#225    mac.doFinal(frameCiphertext)
```

Reachable Packages:
pkg:maven/org.signal/libsignal-client@0.69.1?type=jar
pkg:maven/com.squareup.okio/okio-jvm@3.9.0?type=jar

***#4** Reachable crypto-flow.*

```
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#65    AES/CTR/NoPadding
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#73    iv(new okio.ByteString(iv))
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#81    header.length
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#82    outputStream.write(header)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#147    new BackupFrameOutputStream(fileOutputStream, passphrase)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#152    writeDatabaseVersion(input.getVersion())
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#154    writeDatabaseVersion() ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#155    exportSchema(input, outputStream)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#263    exportSchema(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#174    exportAttachment(attachmentSecret, cursor, outputStream, innerCount, estimatedCount)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#446    exportAttachment(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#178    exportTable(table, input, outputStream, null, null, count, estimatedCount, cancellationSignal)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#383    exportTable(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#166    exportTable(table, input, outputStream, <lambda>, null, count, estimatedCount, cancellationSignal)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#176    exportTable(table, input, outputStream, <lambda>, <lambda>, count, estimatedCount,
cancellationSignal)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#481    exportSticker(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#186    write(preference)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#92    write() ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#191    exportKeyValues(outputStream, SignalStore.getKeysToIncludeInBackup(), count, estimatedCount,
cancellationSignal)
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#533    exportKeyValues(outputStream) ↩
app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#200    write(avatar.getFilename(), inputStream, avatar.getLength())
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#102    write(outputStream, new BackupFrame.Builder().avatar(new
Avatar.Builder().recipientId(avatarName).length(Util.toIntExact(size)).build()).build())
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#212    cipher.update(length)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#213    encryptedLength.length
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#216    mac.update(encryptedLength)
Tags: crypto

app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#217    length = encryptedLength
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#227    out.write(length)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#228    out.write(frameCiphertext)
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#229    out.write(frameMac, 0, 10)
```

```
│ ├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#167    writeStream() ↩
│ ├── core-util/org/signal/core/util/Conversions.java#78    intToByteArray(value) ↩
│ ├── core-util/org/signal/core/util/Conversions.java#80    value >> 8
│ ├── core-util/org/signal/core/util/Conversions.java#81    value >> 16
│ ├── core-util/org/signal/core/util/Conversions.java#82    value >> 24
│ └── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#193    mac.doFinal()
```

Reachable Packages:
pkg:maven/com.squareup.okio/okio-jvm@3.9.0?type=jar

***#5** Reachable crypto-flow.*

```
app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#66    HmacSHA256
├──
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#73    iv(new okio.ByteString(iv))
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#81    header.length
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#82    outputStream.write(header)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#147    new BackupFrameOutputStream(fileOutputStream, passphrase)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#152    writeDatabaseVersion(input.getVersion())
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#154    writeDatabaseVersion() ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#155    exportSchema(input, outputStream)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#263    exportSchema(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#174    exportAttachment(attachmentSecret, cursor, outputStream, innerCount, estimatedCount)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#446    exportAttachment(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#178    exportTable(table, input, outputStream, null, null, count, estimatedCount, cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#383    exportTable(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#166    exportTable(table, input, outputStream, <lambda>, null, count, estimatedCount, cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#176    exportTable(table, input, outputStream, <lambda>, <lambda>, count, estimatedCount,
│   cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#481    exportSticker(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#186    write(preference)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#92    write() ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#191    exportKeyValues(outputStream, SignalStore.getKeysToIncludeInBackup(), count, estimatedCount,
│   cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#533    exportKeyValues(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#200    write(avatar.getFilename(), inputStream, avatar.getLength())
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#208    outputStream.writeEnd()
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#160    writeEnd() ↩
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#161    write(outputStream, new BackupFrame.Builder().end(true).build())
├── core-util/org/signal/core/util/Conversions.java#78    intToByteArray(value) ↩
├── core-util/org/signal/core/util/Conversions.java#80    value >> 8
├── core-util/org/signal/core/util/Conversions.java#81    value >> 16
├── core-util/org/signal/core/util/Conversions.java#82    value >> 24
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#212    cipher.update(length)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#213    encryptedLength.length
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#216    mac.update(encryptedLength)
│   Tags: crypto
│
└── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#225    mac.doFinal(frameCiphertext)
```

Reachable Packages:
pkg:maven/com.squareup.okio/okio-jvm@3.9.0?type=jar

***#6** Reachable crypto-flow.*

```
libsignal-service/org/whispersystems/signalservice/api/crypto/ProfileCipher.java#96    AES
├── new SecretKeySpec(key.serialize(), "AES")
│   Tags: crypto
│
└── libsignal-service/org/whispersystems/signalservice/api/crypto/ProfileCipher.java#98    cipher.doFinal(input, nonce.length, input.length - nonce.length)
    Tags: crypto
```

Reachable Packages:
pkg:maven/org.signal/libsignal-client@0.69.1?type=jar

***#7** 2 packages reachable from this crypto-flow.*

```
app/org/thoughtcrime/securesms/backup/FullBackupBase.java#20    SHA-512
├── app/org/thoughtcrime/securesms/backup/FullBackupBase.java#24    digest.update(salt)
│   Tags: crypto
│
├── app/org/thoughtcrime/securesms/backup/FullBackupBase.java#27    digest.update(hash)
│   Tags: crypto
│
├── app/org/thoughtcrime/securesms/backup/FullBackupBase.java#28    digest.digest(input)
│   Tags: crypto
│
├── app/org/thoughtcrime/securesms/backup/FullBackupBase.java#31    ByteUtil.trim(hash, 32)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#58    getBackupKey(passphrase, salt)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#59    HKDF.deriveSecrets(key, "Backup Export".getBytes(), 64)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#60    ByteUtil.split(derived, 32, 32)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#62    split[0]
├──
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#73    iv(new okio.ByteString(iv))
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#81    header.length
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#82    outputStream.write(header)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#147    new BackupFrameOutputStream(fileOutputStream, passphrase)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#152    writeDatabaseVersion(input.getVersion())
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#154    writeDatabaseVersion() ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#155    exportSchema(input, outputStream)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#263    exportSchema(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#174    exportAttachment(attachmentSecret, cursor, outputStream, innerCount, estimatedCount)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#446    exportAttachment(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#178    exportTable(table, input, outputStream, null, null, count, estimatedCount, cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#383    exportTable(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#166    exportTable(table, input, outputStream, <lambda>, null, count, estimatedCount, cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#176    exportTable(table, input, outputStream, <lambda>, <lambda>, count, estimatedCount,
│   cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#481    exportSticker(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#186    write(preference)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#92    write() ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#191    exportKeyValues(outputStream, SignalStore.getKeysToIncludeInBackup(), count, estimatedCount,
│   cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#533    exportKeyValues(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#200    write(avatar.getFilename(), inputStream, avatar.getLength())
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#208    outputStream.writeEnd()
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#160    writeEnd() ↩
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#161    write(outputStream, new BackupFrame.Builder().end(true).build())
├── core-util/org/signal/core/util/Conversions.java#78    intToByteArray(value) ↩
├── core-util/org/signal/core/util/Conversions.java#80    value >> 8
├── core-util/org/signal/core/util/Conversions.java#81    value >> 16
├── core-util/org/signal/core/util/Conversions.java#82    value >> 24
```

```
└── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#220    doFinal(frame.encode())
```

Reachable Packages:
pkg:maven/org.signal/libsignal-client@0.69.1?type=jar
pkg:maven/com.squareup.okio/okio-jvm@3.9.0?type=jar

***#8** 2 packages reachable from this crypto-flow.*

```
app/org/thoughtcrime/securesms/backup/FullBackupBase.java#20    SHA-512
├── app/org/thoughtcrime/securesms/backup/FullBackupBase.java#24    digest.update(salt)
│   Tags: crypto
│
├── app/org/thoughtcrime/securesms/backup/FullBackupBase.java#27    digest.update(hash)
│   Tags: crypto
│
├── app/org/thoughtcrime/securesms/backup/FullBackupBase.java#28    digest.digest(input)
│   Tags: crypto
│
├── app/org/thoughtcrime/securesms/backup/FullBackupBase.java#31    ByteUtil.trim(hash, 32)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#58    getBackupKey(passphrase, salt)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#59    HKDF.deriveSecrets(key, "Backup Export".getBytes(), 64)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#60    ByteUtil.split(derived, 32, 32)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#62    split[0]
├──
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#73    iv(new okio.ByteString(iv))
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#81    header.length
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#82    outputStream.write(header)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#147    new BackupFrameOutputStream(fileOutputStream, passphrase)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#152    writeDatabaseVersion(input.getVersion())
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#154    writeDatabaseVersion() ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#155    exportSchema(input, outputStream)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#263    exportSchema(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#174    exportAttachment(attachmentSecret, cursor, outputStream, innerCount, estimatedCount)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#446    exportAttachment(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#178    exportTable(table, input, outputStream, null, null, count, estimatedCount, cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#383    exportTable(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#166    exportTable(table, input, outputStream, <lambda>, null, count, estimatedCount, cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#176    exportTable(table, input, outputStream, <lambda>, <lambda>, count, estimatedCount,
│   cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#481    exportSticker(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#186    write(preference)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#92    write() ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#191    exportKeyValues(outputStream, SignalStore.getKeysToIncludeInBackup(), count, estimatedCount,
│   cancellationSignal)
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#533    exportKeyValues(outputStream) ↩
├── app/org/thoughtcrime/securesms/backup/FullBackupExporter.java#200    write(avatar.getFilename(), inputStream, avatar.getLength())
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#102    write(outputStream, new BackupFrame.Builder().avatar(new
│   Avatar.Builder().recipientId(avatarName).length(Util.toIntExact(size)).build()).build())
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#212    cipher.update(length)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#213    encryptedLength.length
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#216    mac.update(encryptedLength)
│   Tags: crypto
│
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#217    length = encryptedLength
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#227    out.write(length)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#228    out.write(frameCiphertext)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#229    out.write(frameMac, 0, 10)
├── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#167    writeStream() ↩
├── core-util/org/signal/core/util/Conversions.java#78    intToByteArray(value) ↩
├── core-util/org/signal/core/util/Conversions.java#80    value >> 8
├── core-util/org/signal/core/util/Conversions.java#81    value >> 16
├── core-util/org/signal/core/util/Conversions.java#82    value >> 24
└── app/org/thoughtcrime/securesms/backup/BackupFrameOutputStream.java#189    cipher.doFinal()
```

Reachable Packages:
pkg:maven/org.signal/libsignal-client@0.69.1?type=jar
pkg:maven/com.squareup.okio/okio-jvm@3.9.0?type=jar

***#9** Reachable crypto-flow.*

```
libsignal-service/org/whispersystems/signalservice/api/crypto/UnidentifiedAccess.java#58    AES
├── new SecretKeySpec(profileKey.serialize(), "AES")
│   Tags: crypto
│
├── libsignal-service/org/whispersystems/signalservice/api/crypto/UnidentifiedAccess.java#60    cipher.doFinal(input)
│   Tags: crypto
│
├── libsignal-service/org/whispersystems/signalservice/api/crypto/UnidentifiedAccess.java#62    ByteUtil.trim(ciphertext, 16)
├── libsignal-service/org/whispersystems/signalservice/api/crypto/ProfileCipher.java#190    UnidentifiedAccess.deriveAccessKeyFrom(key)
├── libsignal-service/org/whispersystems/signalservice/api/crypto/ProfileCipher.java#193    new SecretKeySpec(unidentifiedAccessKey, "HmacSHA256")
│   Tags: crypto
│
└── libsignal-service/org/whispersystems/signalservice/api/crypto/ProfileCipher.java#195    mac.doFinal(new byte[32])
    Tags: crypto
```

Reachable Packages:
pkg:maven/org.signal/libsignal-client@0.69.1?type=jar

***#10** Reachable crypto-flow.*

```
libsignal-service/org/whispersystems/signalservice/api/crypto/UnidentifiedAccess.java#57    AES/GCM/NoPadding
├── libsignal-service/org/whispersystems/signalservice/api/crypto/UnidentifiedAccess.java#58    cipher.init(Cipher.ENCRYPT_MODE, new SecretKeySpec(profileKey.serialize(),
│   "AES"), new GCMParameterSpec(128, nonce))
│   Tags: crypto
│
├── libsignal-service/org/whispersystems/signalservice/api/crypto/UnidentifiedAccess.java#60    cipher.doFinal(input)
│   Tags: crypto
│
├── libsignal-service/org/whispersystems/signalservice/api/crypto/UnidentifiedAccess.java#62    ByteUtil.trim(ciphertext, 16)
├── libsignal-service/org/whispersystems/signalservice/api/crypto/ProfileCipher.java#190    UnidentifiedAccess.deriveAccessKeyFrom(key)
├── libsignal-service/org/whispersystems/signalservice/api/crypto/ProfileCipher.java#193    new SecretKeySpec(unidentifiedAccessKey, "HmacSHA256")
│   Tags: crypto
│
└── libsignal-service/org/whispersystems/signalservice/api/crypto/ProfileCipher.java#195    mac.doFinal(new byte[32])
    Tags: crypto
```

Reachable Packages:
pkg:maven/org.signal/libsignal-client@0.69.1?type=jar

Secure Design Tips

- Generate a Cryptographic BOM with cdxgen and monitor it in Dependency-Track.