COMMUNITY
THE ASF CONFERENCE
CODE

The Jagged Edge

Streaming End-to-End Encryption with age in Java and Beyond

David Handermann, PMC Member of Apache NiFi, Software Engineer at Datavolo

Introduction – David Handermann

PMC Member
nifi.apache.org

Software Engineer
datavolo.io

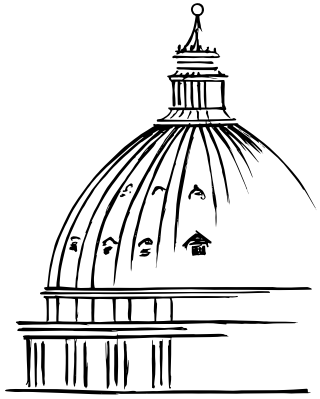
Software Development Blog
exceptionfactory.com

Introduction

Review of **age encryption**

1. What is age encryption?
2. What is Jagged?
3. Where is age available?

What is age encryption?



age

FILE ENCRYPTION

Modern file encryption format

with pluggable recipients

What is age encryption?

Open Specification: **Authors and Features**

- Prounounced with a hard **g**
- Authors: **Filippo Valsorda** and **Ben Cartwright-Cox**
- Reference API and CLI in **Go**
- Streaming **authenticated encryption**
- **Public key** or **password-based** recipients

What is age encryption?

Open Specification: **age-encryption.org/v1**

- One cipher algorithm: **ChaCha20-Poly1305**
- One native public key algorithm: **X25519**
- One native password algorithm: **scrypt**
- One extension point: **Recipient Type**
- Two file encodings: **Binary** and **Base64**

What is age encryption?

Open Specification: **Test Vectors**

- Community Cryptography Test Vectors
  - **github.com/C2SP/CCTV**
- Over 100 positive and negative test cases
- Covers expected error conditions

What is age encryption?

Open Specification: **Why age?**

- Alternative to **OpenPGP** for **file encryption**
- Support **streamable** encryption and decryption
- Standardize on **modern algorithms**
- Support integration with **SSH public keys**
- Avoid algorithm negotation issues

What is age encryption?

age and **age-keygen**

Simple CLI

What is age encryption?

Simple Commands: **age-keygen**

```
$ age-keygen -o private.key

Public key: age1ql3z7hjy54...
```

What is age encryption?

Simple Commands: **age** encryption

```
$ age -e \
      -r age1ql3z7hjy54... \
      -o data.age \
      data
```

What is age encryption?

Simple Commands: **age** decryption

```
$ age -d \
      -i private.key \
      -o data \
      data.age
```

What is age encryption?

File Format: **Header lines**

```
age-encryption.org/v1
-> X25519 Xel0dJ6y3C7...
qRS0AMjdjPvZ/WT08U2KL...
--- HK2NmOBN9Dpq0Gw6x...
```

What is age encryption?

File Format: **Header fields**

Version: `age-encryption.org/v1`

Recipient Stanza: `-> X25519 Xe10d...`

Header MAC: `--- HK2NmOBN9Dpq0G...`

What is age encryption?

File Format: **Binary Payload**

- Starts with **random nonce** of **16 bytes**
- One or more **chunks** of up to **64 KiB**
  - Encrypted with **payload key**
  - Incremental **nonce** with **chunk counter**

What is Jagged?

Jagged

age Encryption in Java

What is Jagged?

Java Implementation: **age in Java**

- Supports Java 11 through 21 with **no dependencies**
- Supports Java 8 with **Bouncy Castle Provider**
- Comprehensive unit tests and test vectors

github.com/exceptionfactory/jagged

What is Jagged?

Java Implementation: **Modular design**

- **jagged-api** and **jagged-framework**
- Recipient Type modules
  - **jagged-scrypt**
  - **jagged-ssh**
  - **jagged-x25519** with **jagged-bech32**

What is Jagged?

Java Implementation: **What is Bech32?**

- **Base32** encoding
- Bitcoin Improvement Proposal 173
  - **Human Readable Part** indicating data type
  - **Separator** always the character **1**
  - **Data Part** with **checksum** of six characters

What is Jagged?

Java Implementation: **Key pair generation**

```
KeyPairGenerator generator = new X25519KeyPairGenerator();
KeyPair keyPair = generator.generateKeyPair();

PublicKey publicKey = keyPair.getPublic();
System.out.printf("Public key: %s", publicKey);
```

```
Public key: age1ql3z7hjy54pw3hyww5ayyfg7zqgvc7...
```

What is Jagged?

Java Implementation: **Java NIO**

- Encrypt using **WritableByteChannel**
  - Armored or Standard EncryptingChannelFactory
- Decrypt using **ReadableByteChannel**
  - Armored or Standard DecryptingChannelFactory

What is Jagged?

Java Implementation: **Recipient Types**

- Encrypt using **RecipientStanzaWriter**
- Decrypt using **RecipientStanzaReader**

What is Jagged? Binary encryption with X25519 Public Key

```
CharSequence key = getPublicKey();
RecipientStanzaWriter writer = newRecipientStanzaWriter(key);
EncryptingChannelFactory factory = new StandardEncryptingChannelFactory();

try (
    ReadableByteChannel inputChannel = Files.newByteChannel(...);
    WritableByteChannel outputChannel = factory.newEncryptingChannel(
        Files.newByteChannel(...),
        List.of(writer)
    );
) {
    copy(inputChannel, outputChannel);
}
```

Where is age available?

Multiple **platforms**

Multiple **languages**

Multiple **projects**

Where is age available?

Multiple Platforms: **Standard CLI packages**

- **macOS**: brew install age
- **Debian and Ubuntu**: apt install age
- **Windows**: choco install age.portable
- Most Linux distributions

Where is age available?

Multiple Languages: **Implementation libraries**

- **Go**: age
- **Java**: Jagged
- **Rust**: rage
- **Python**: pyrage
- **TypeScript**: typage
- **Dart**: dage
- **Elixir**: age_ex
- **Kotlin**: kage
- **Swift**: AgeKit
- **WebAssembly**: wage

Where is age available?

Multiple Projects: **Integrations**

- **age-online.com** WebAssembly user interface
- **passage** password-store using age
- **SOPS** editor for encrypted structured configuration
- **Apache NiFi** Processors

Where is age available?

Multiple Projects: **Apache NiFi Processors**

- **EncryptContentAge** with public keys
- **DecryptContentAge** with private keys
- NiFi **Parameter Providers** for externalized keys
- Released in NiFi 1.24.0 and 2.0.0-M1

Conclusion

age encryption

open

modern

streaming

Conclusion

Jagged

github.com/exceptionfactory/jagged

Conclusion

Stay connected

exceptionfactory.com