KIP-573: Enable TLSv1.3 by default

Status

Current state: *Accepted*

Discussion thread: *here*

JIRA: KAFKA-9320

Motivation

This KIP is follow-up for the KIP-553

In KAFKA-7251 support of TLS1.3 was introduced.

For now, only TLS1.2 and TLS1.3 are recommended for the usage, other versions of TLS considered as obsolete:

- https://www.rfc-editor.org/info/rfc8446
- https://en.wikipedia.org/wiki/Transport_Layer_Security#History_and_development

Testing of TLS1.3 was completed in KAFKA-9319

We should enable actual versions of the TLS protocol by default to provide to the users only secure implementations.

Users can enable obsolete versions of the TLS with the configuration if they want to.

We can't use only TLSv1.3 because the support of it was introduced in JDK11 - https://docs.oracle.com/en/java/javase/11/security/java-secure-socket-extension-jsse-reference-guide.html#GUID-F069F4ED-DF2C-4B3B-90FB-F89E700CF21A.

Public Interfaces

There are no changes in public interfaces.

Proposed Changes

If Kafka started on java11 compatible environment then

```
SslConfigs.DEFAULT_SSL_ENABLED_PROTOCOLS = "TLSv1.2,TLSv1.3"
```

```
SslConfigs.DEFAULT_SSL_PROTOCOL = "TLSv1.3"
```

If Kafka started on java version that is lower java11 then

```
SslConfigs.DEFAULT_SSL_ENABLED_PROTOCOLS = "TLSv1.2"
```

```
SslConfigs.DEFAULT_SSL_PROTOCOL = "TLSv1.2"
```

Compatibility, Deprecation, and Migration Plan

Compatibility: There are no compatibility issues.

Migration: Users who are using TLSv1.1 and TLSv1 should enable these versions of the protocol with the explicit configuration property `"ssl.enabled.protocols"`

TLSv1.3 will not work for users who configured cipher suite explicitly - one needs to update the list of ciphers to include TLSv1.3 ciphers which use a different naming convention. The client will downgrade to TLS 1.2 in this case.

Rejected Alternatives

Wait until java8 gets TLSv1.3 support and made changes afterward.