FAPI-SIG Community 29th Meeting

@Web Conference

27 Oct 2021

PROPOSED DRAFT

Table of Contents

Major Topics

Discussion :

- Revised Client Policies
- FAPI 2.0 Baseline

Working Items Status

Major Topics

Major Topics

- Self contained access token specification has been published

  RFC 9068 JSON Web Token (JWT) Profile for OAuth 2.0 Access Token

  https://datatracker.ietf.org/doc/html/rfc9068

  Does keycloak need to follow this specification?

  Ex. an access token’s JOSE header “typ” field should be “at+jwt”

  keycloak discussion :

  https://github.com/keycloak/keycloak/discussions/8646

Discussion : Revising Client Policies

Decide whether a condition/executor is applied or not based on event

[JIRA Ticket]

- KEYCLOAK-19597 Make ClientPolicyContext more rich to avoid editing all conditions/executors when introduce new event type
  https://issues.redhat.com/browse/KEYCLOAK-19597

[Current Situation]

- A condition and executor decides whether it is applied or not based on an event (ClientPolicyEvent).
- A new event type may be introduced in the future.

[Problem]

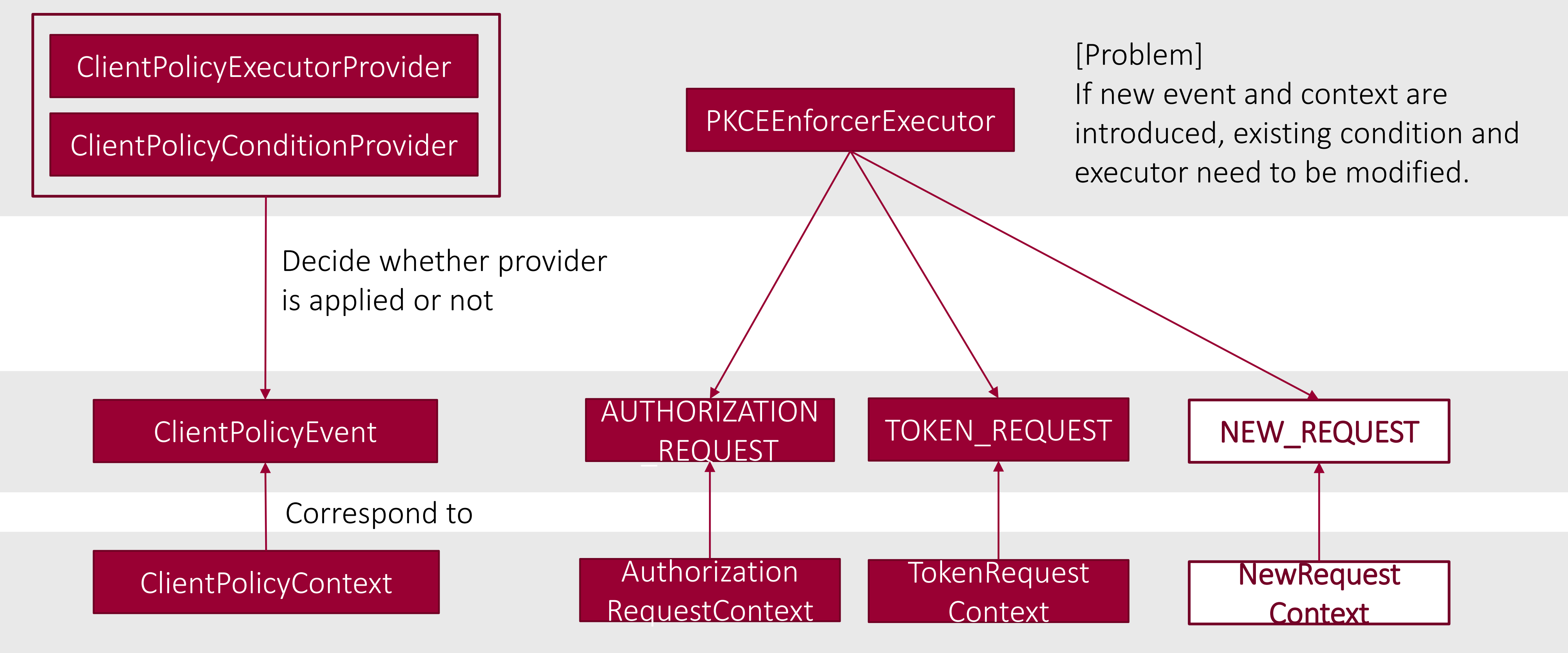
- If new event and context is introduced, existing condition and executor need to be modified.

-> Increasing keycloak maintenance cost.

[Solution]

- Introduce context(ClientPolicyContext)'s metadata.
- A condition and executor decides whether it is applied or not based on context(ClientPolicyContext)'s metadata, not directly an event (ClientPolicyEvent).

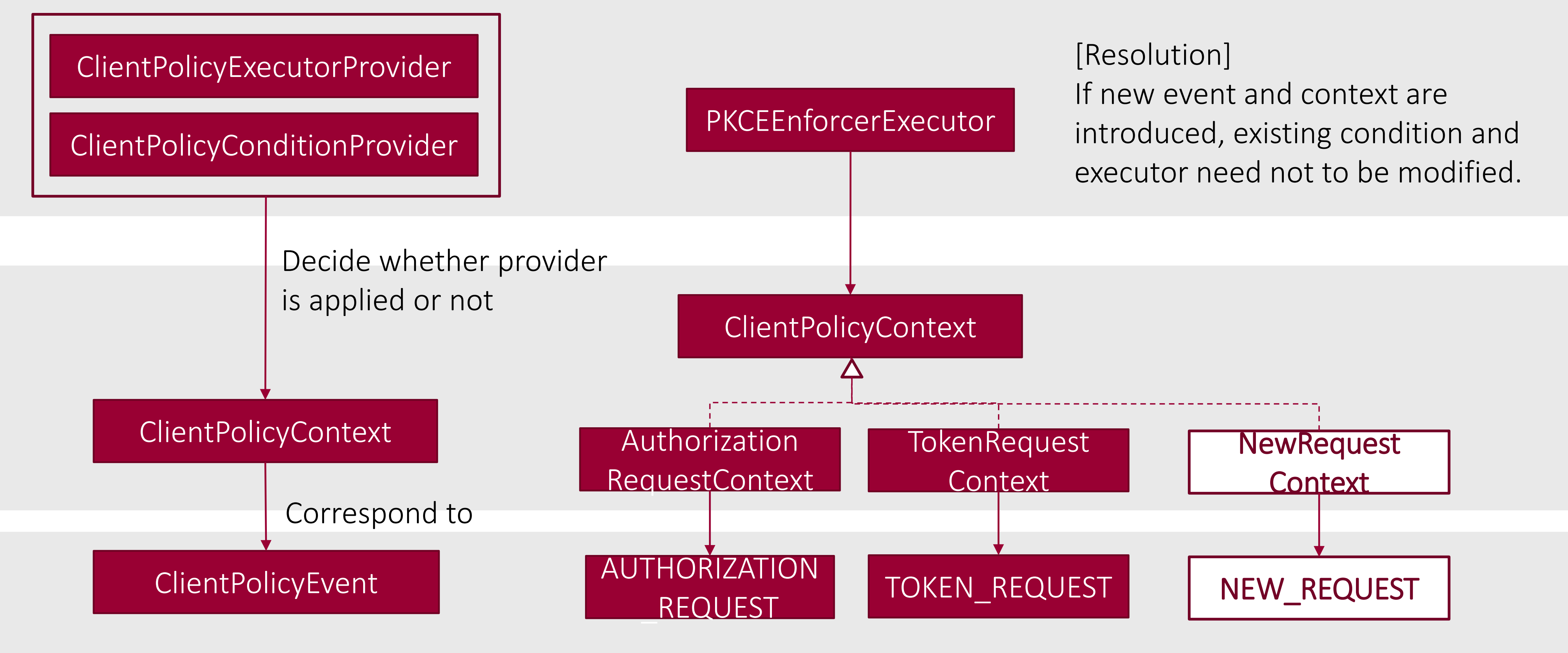
Decide whether a provider is applied or not Based on event



[Problem]
If new event and context are introduced, existing condition and executor need to be modified.

PROPOSED DRAFT

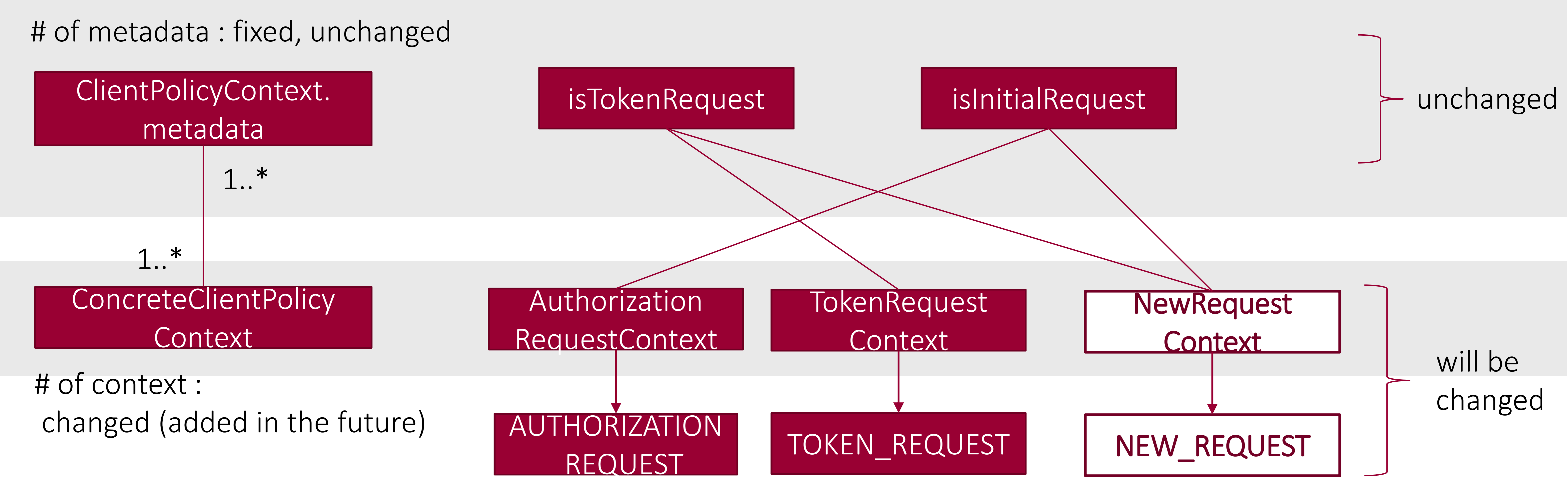
Decide whether a provider is applied or not Based on context’s metadata



[Resolution]
If new event and context are introduced, existing condition and executor need not to be modified.

PROPOSED DRAFT

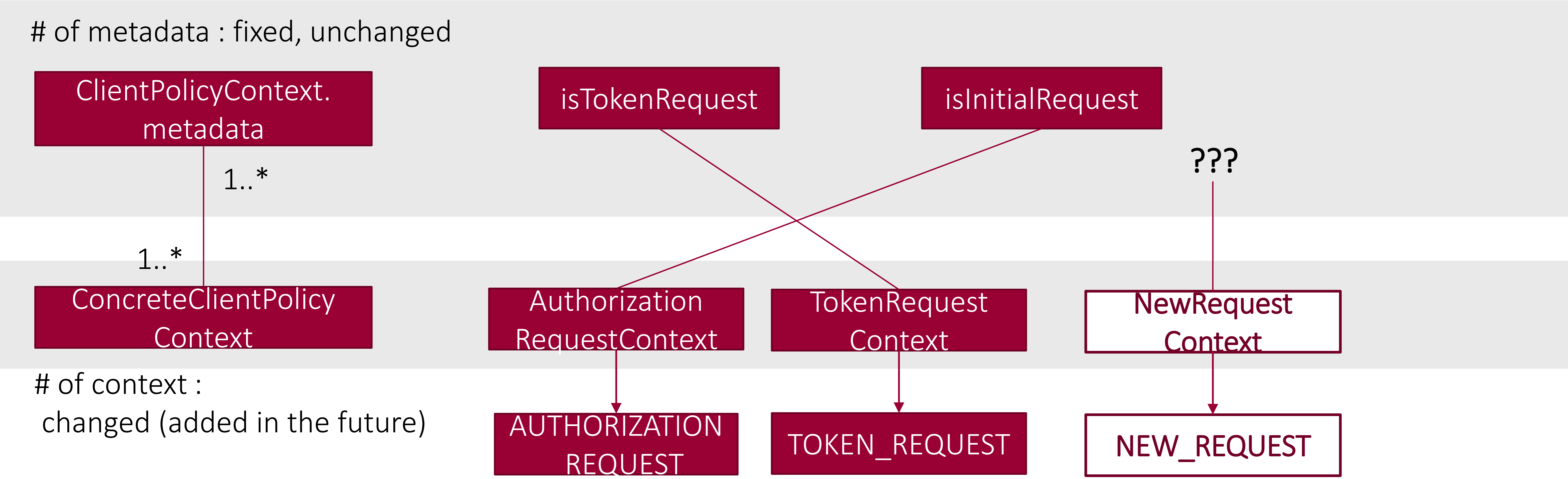
Decide whether a provider is applied or not Based on context's metadata



- Variable part is degenerated to fixed part.
- Part (executor/condition) relying on fixed part remains unchanged.

PROPOSED DRAFT

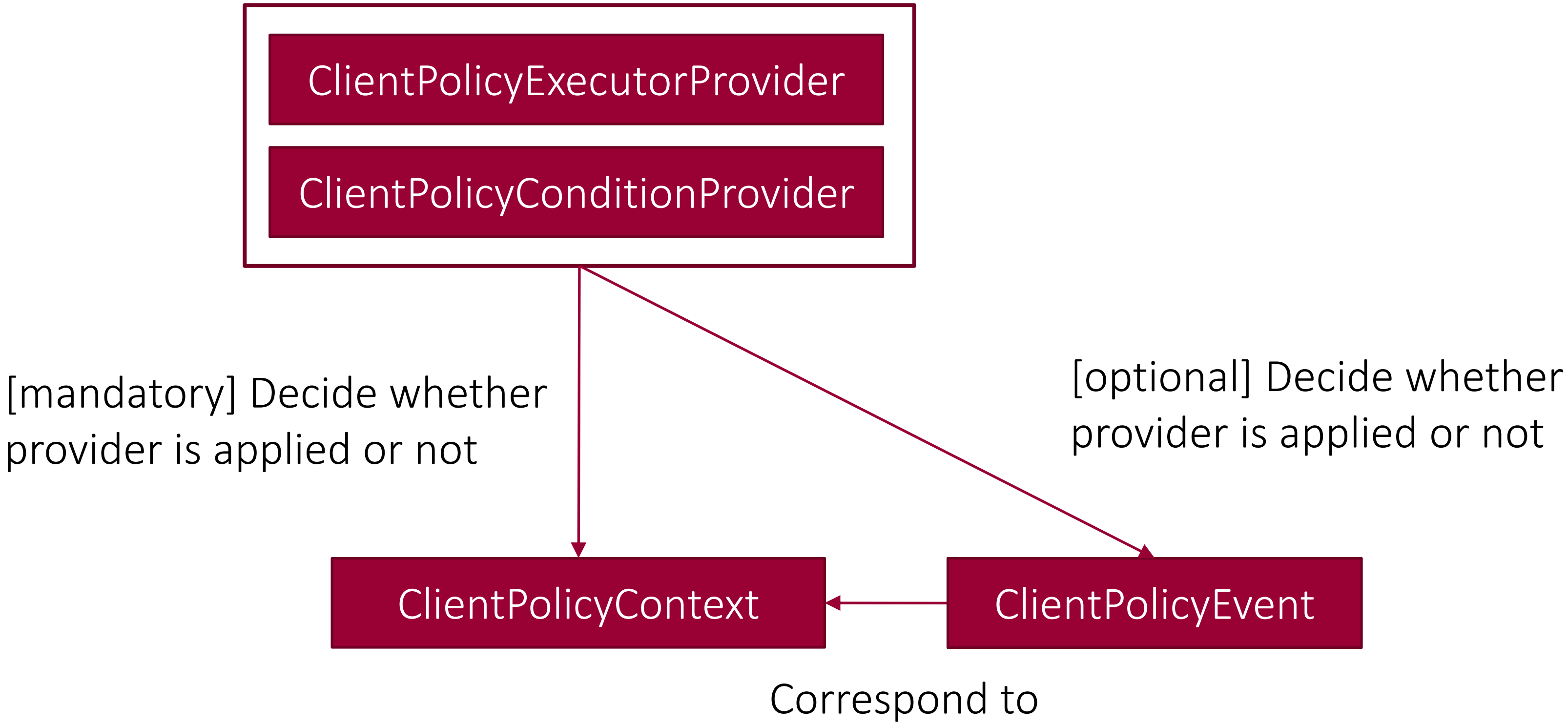
Decide whether a provider is applied or not Based on context’s metadata



# of metadata : fixed, unchanged
ClientPolicyContext.metadata
isTokenRequest
isInitialRequest
???
1..*
1..*
ConcreteClientPolicyContext
AuthorizationRequestContext
TokenRequestContext
NewRequestContext
# of context :
changed (added in the future)
AUTHORIZATION REQUEST
TOKEN_REQUEST
NEW_REQUEST

- Newly added context may not correspond to any context’s metadata.

Decide whether a provider is applied or not Compromise



ClientPolicyExecutorProvider

ClientPolicyConditionProvider

[mandatory] Decide whether provider is applied or not

[optional] Decide whether provider is applied or not

ClientPolicyContext

ClientPolicyEvent

Correspond to

PROPOSED DRAFT

Discussion : FAPI 2.0 Baseline

FAPI 2.0 Baseline (Draft ver)

Supported #1 : Server Metadata Advertisement

Possible #2 : Accept Authorization Code Grant

Currently, it has already been achieved by client settings, not client policies.

In Progress #3 : Reject Implicit Grant and Resource Owner Password Credentials Grant

Currently, it has already been achieved by client settings, not client policies.

PR sent KEYCLOAK-19539 FAPI 2.0 Baseline : Reject Implicit Grant

https://github.com/keycloak/keycloak/pull/8574

Merged KEYCLOAK-19540 FAPI 2.0 Baseline : Reject Resource Owner Password Credentials Grant

https://github.com/keycloak/keycloak/pull/8589

Possible #4 : Accept PAR

Currently, it has already been achieved by client settings, not client policies.

FAPI 2.0 Baseline (Draft ver)

Possible #5 : Reject authorization request except PAR

Currently, it has already been achieved by client settings, not client policies.

Supported #6 : Reject PAR without client authentication

Client is authenticated on PAR endpoint as default.

FAPI 2.0 Baseline (Draft ver)

In Progress #7 : PAR’s authorization_details support

Supported #8 : Accept only confidential client

Supported #9 : Holder-of-Key token support

Currently, it has already been achieved by mutual TLS. DPoP is under development.

Supported #10 : Accept only specified secure client authentication methods

Supported #11 : Require PKCE

Not Yet #12 : Require PAR including redirect_uri

Not Yet #13 : Require authorization response including iss

Not Yet #14 : Make sure TLS for HTTP redirect with authorization response

Supported #15 : Detect multiple use of authorization code

Supported NOTE section’s description.

FAPI 2.0 Baseline (Draft ver)

Supported #16 : Provide mechanism for verifying access token by resource server

Supported #17 : Prohibit 307 redirect

Optional #18 : Should use 303 redirect

Supported #19 : Prohibit Open Redirector

Supported #20 : Check aud claim’s value of JWS client assertion in private_key_jwt

Currently, JWTClientAuthenticator supported it.

Difference between FAPI2 and FAPI1

#1 : Not require JAR and JARM

#2 : Require RAR

#3 : Not require s_hash

#4 : Require redirect_uri in PAR

#5 : Not require hybrid flow

#6 : Not require ID token as detached signature

#7 : Not require JWE for ID token

#8 : Add DPoP for Holder-of-Key token

Working Items Status

Working Items

[Security Features]

<Common>

In Progress OIDC Client’s Public Key Management — Hitachi

1st phase -> 2nd phase

In Progress Revising Client Policies — Hitachi

[Security Features]

<SPA/Native App>

In Progress OAuth 2.0 Demonstration of Proof-of-Possession (DPoP) — Backbase

Working Items

[Security Features]

<High Level Security>

● FAPI 2.0 (baseline/advanced)

In Progress	Rich Authorization Request (RAR)	🇩🇪 🇺🇦 Adorsys
In Progress	Grant Management API	🇩🇪 🇺🇦 Adorsys
In Progress	Other requirements support	🇯🇵 Hitachi

Working Items

[Market Specific Features]

<PSD2>

- ● Following eIDAS regulations

In Progress QWAC verification

Adorsys

- ● Consent Management

<UK OpenBanking>

- ● Onboarding
  - Software Statement Support
  - Software Statement Assertion (SSA) Verification

Roadmap

Security	2020 Sep	2021 Apr
Common Client Policies	• Implemented as Preview • New Admin REST API support	• Migrate Client Registration Policy • Move Preview to Official Support -> leads to FAPI 1.0 Official Support
High Level Security		
FAPI 1.0	• Supported ID2 ver • Passed ID2 conformance test	• Support Final ver • Pass Final ver conformance test
FAPI 2.0		• Start design and implementation PAR, RAR, Grant Management API
FAPI-CIBA	• Supported Pure CIBA (poll mode) as Preview	• Support FAPI-CIBA (poll mode) • Pass conformance test
SPA/Native App DPoP		• Start design and implementation

PROPOSED DRAFT

Roadmap

Market Specific	2020 Sep	2021 Apr
PSD2	- Discussed QWAC verification	- Start design and implementation QWAC verification
UK OpenBanking		- Start design and implementation (?) Onboarding
Open Banking Brasil		- Support OBB FAPI

END