Insecure Direct Object Reference

(IDOR)

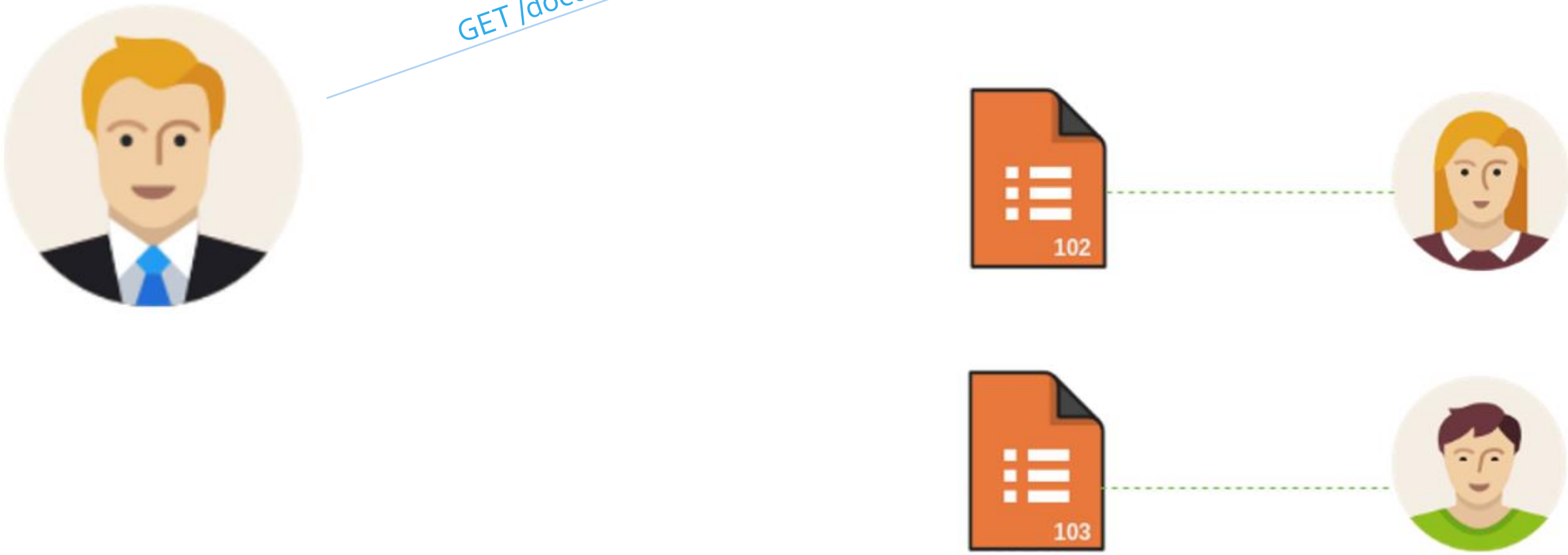
IDOR

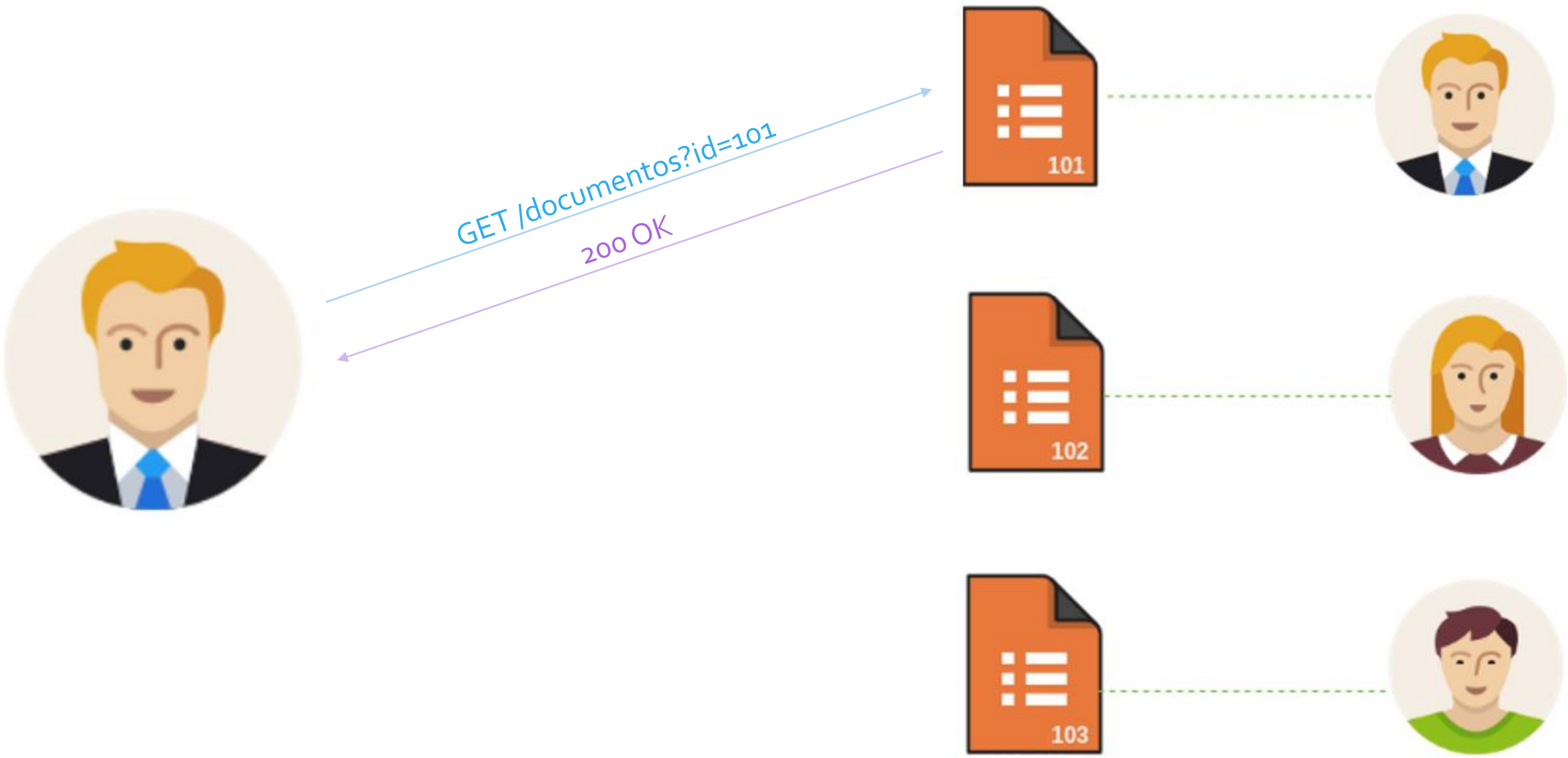
- Este tipo de vulnerabilidad puede ocurrir cuando un servidor web recibe una entrada proporcionada por el usuario para recuperar objetos (archivos, datos, documentos), se ha depositado demasiada confianza en los datos de entrada y no se valida en el lado del servidor si objeto solicitado pertenece al usuario que lo solicita.

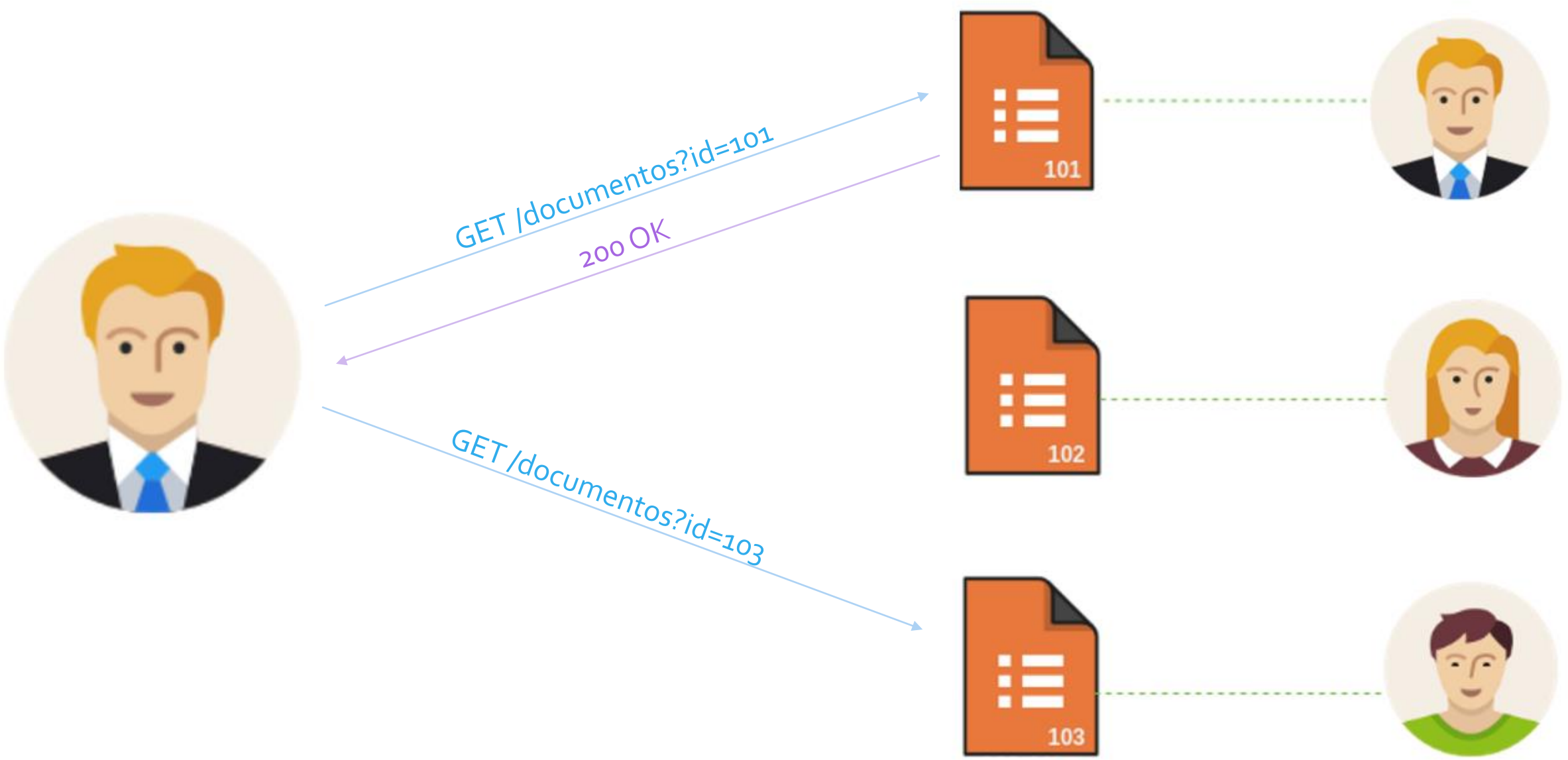

101

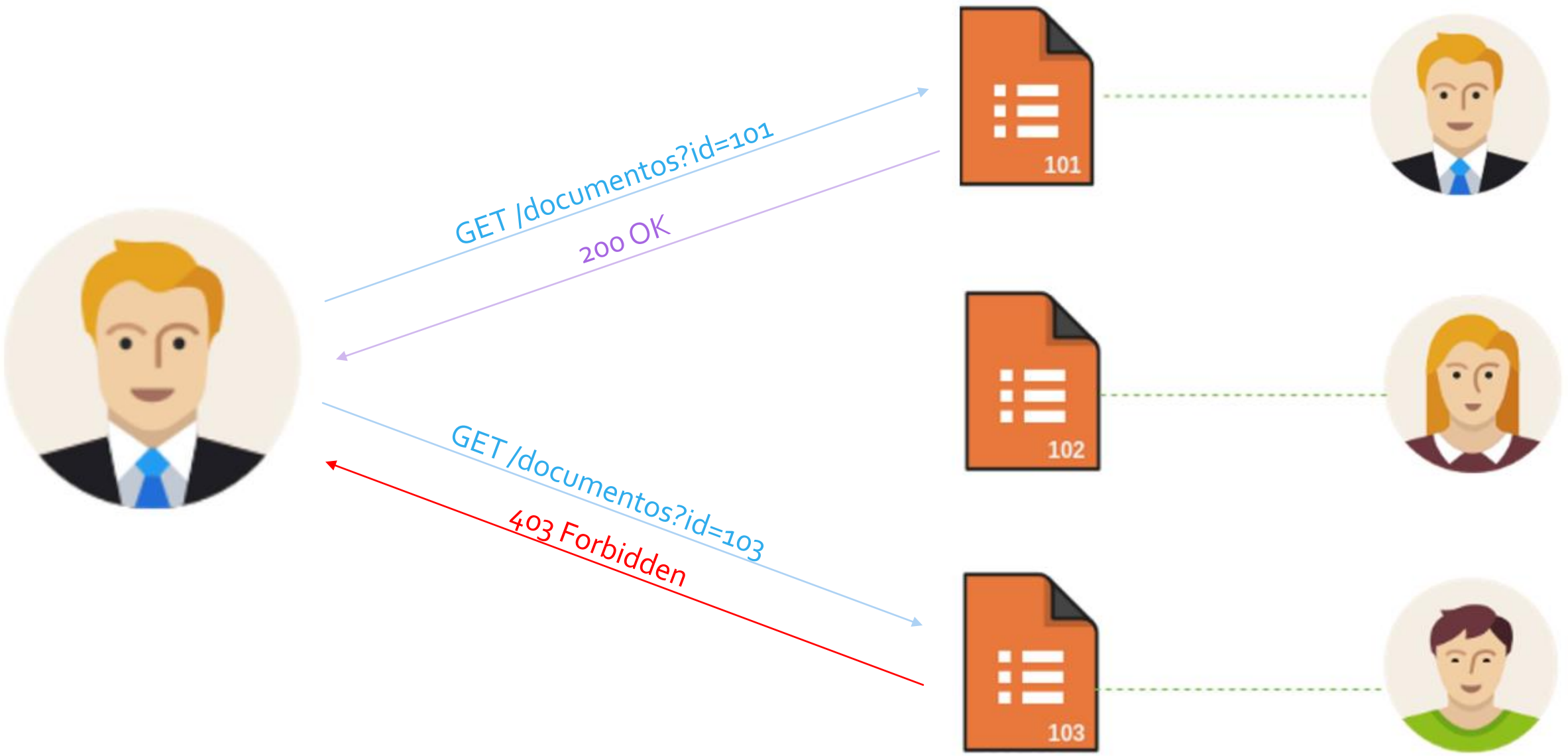

102

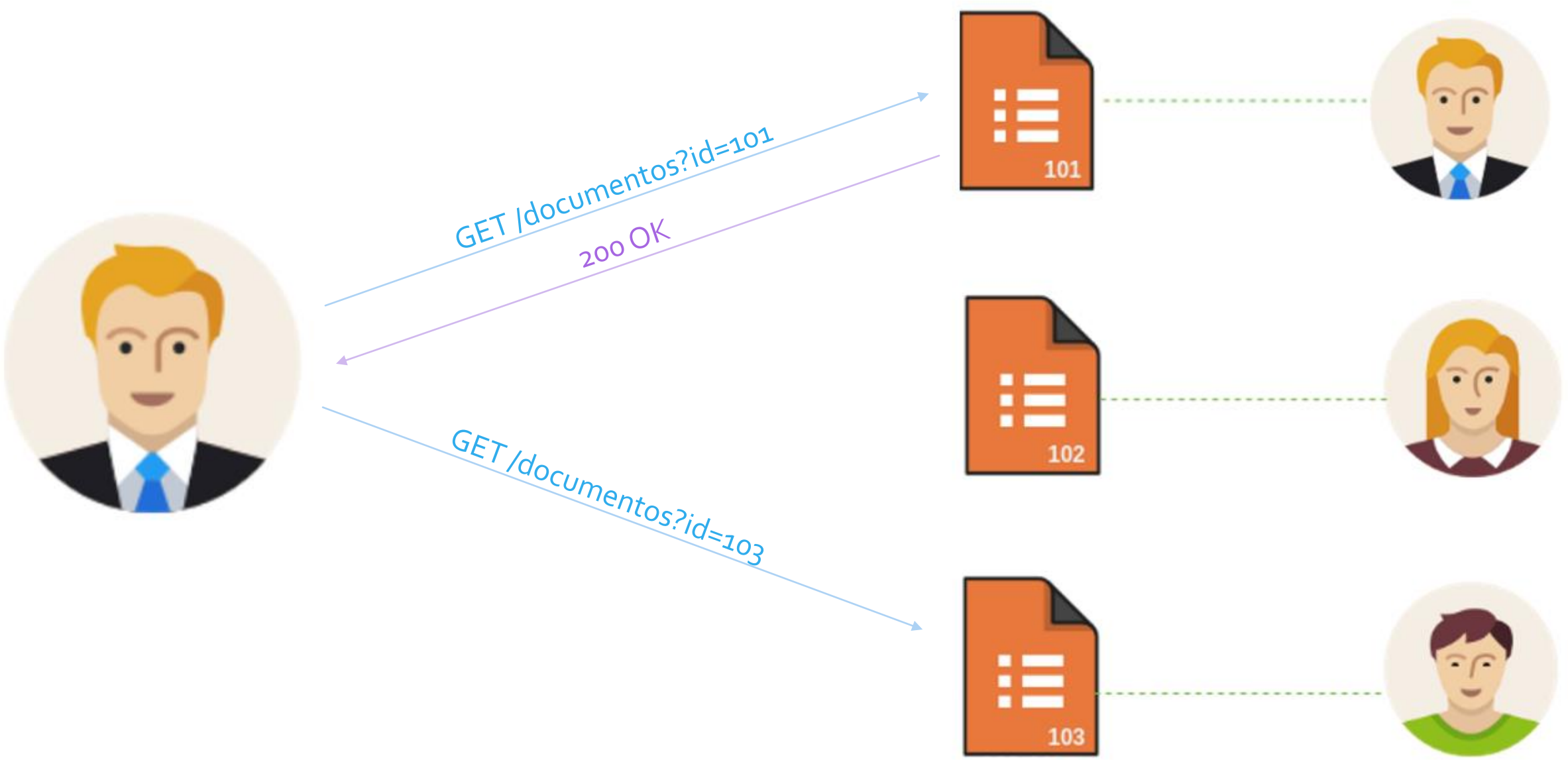

103

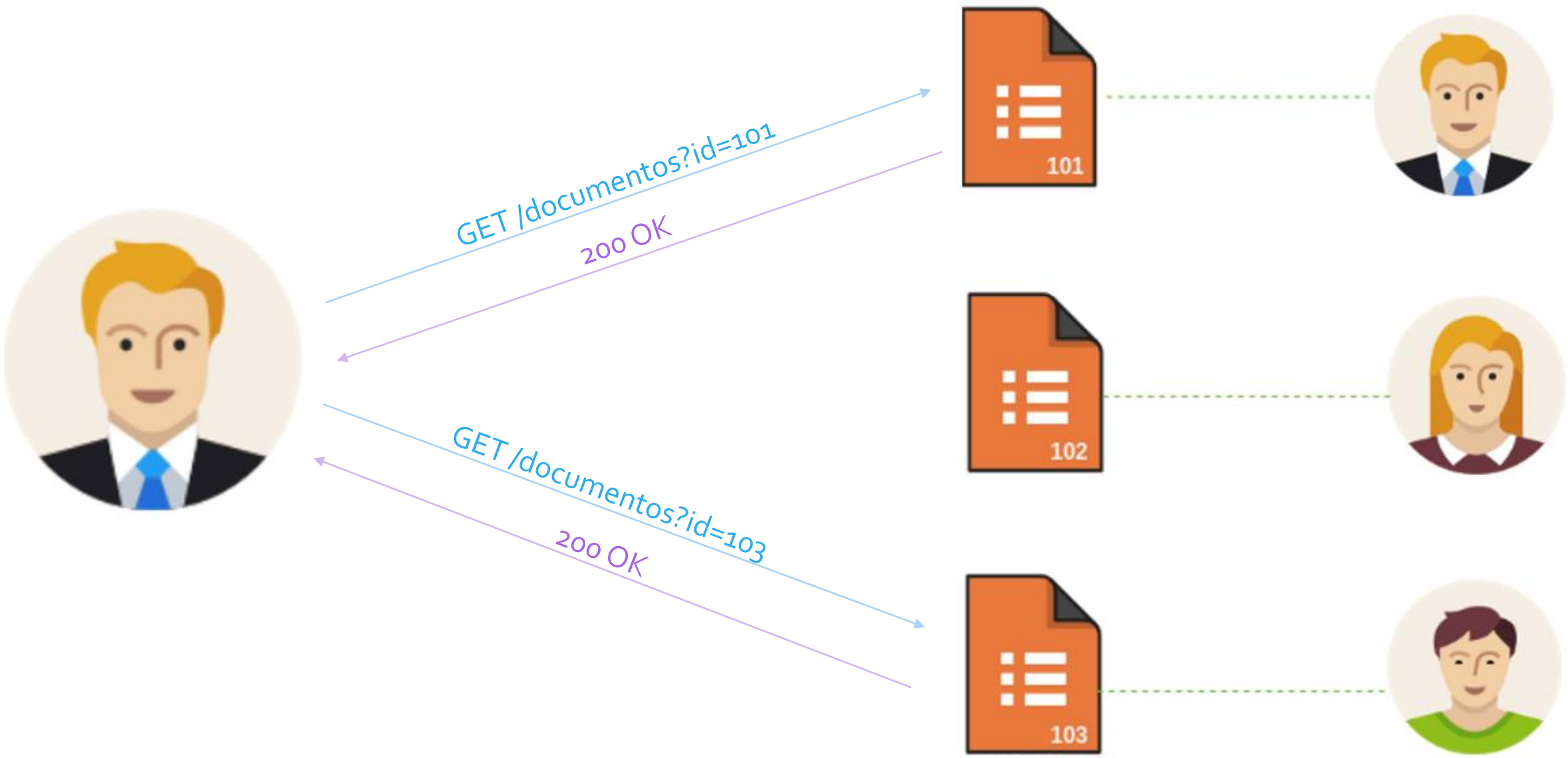

GET /documentos?id=101
101
102
103


GET /documentos?id=101
200 OK
101
102
103


GET /documentos?id=101
200 OK
GET /documentos?id=103
101
102
103


GET /documentos?id=101
200 OK
GET /documentos?id=103
403 Forbidden
101
102
103


GET /documentos?id=101
200 OK
GET /documentos?id=103
101
102
103

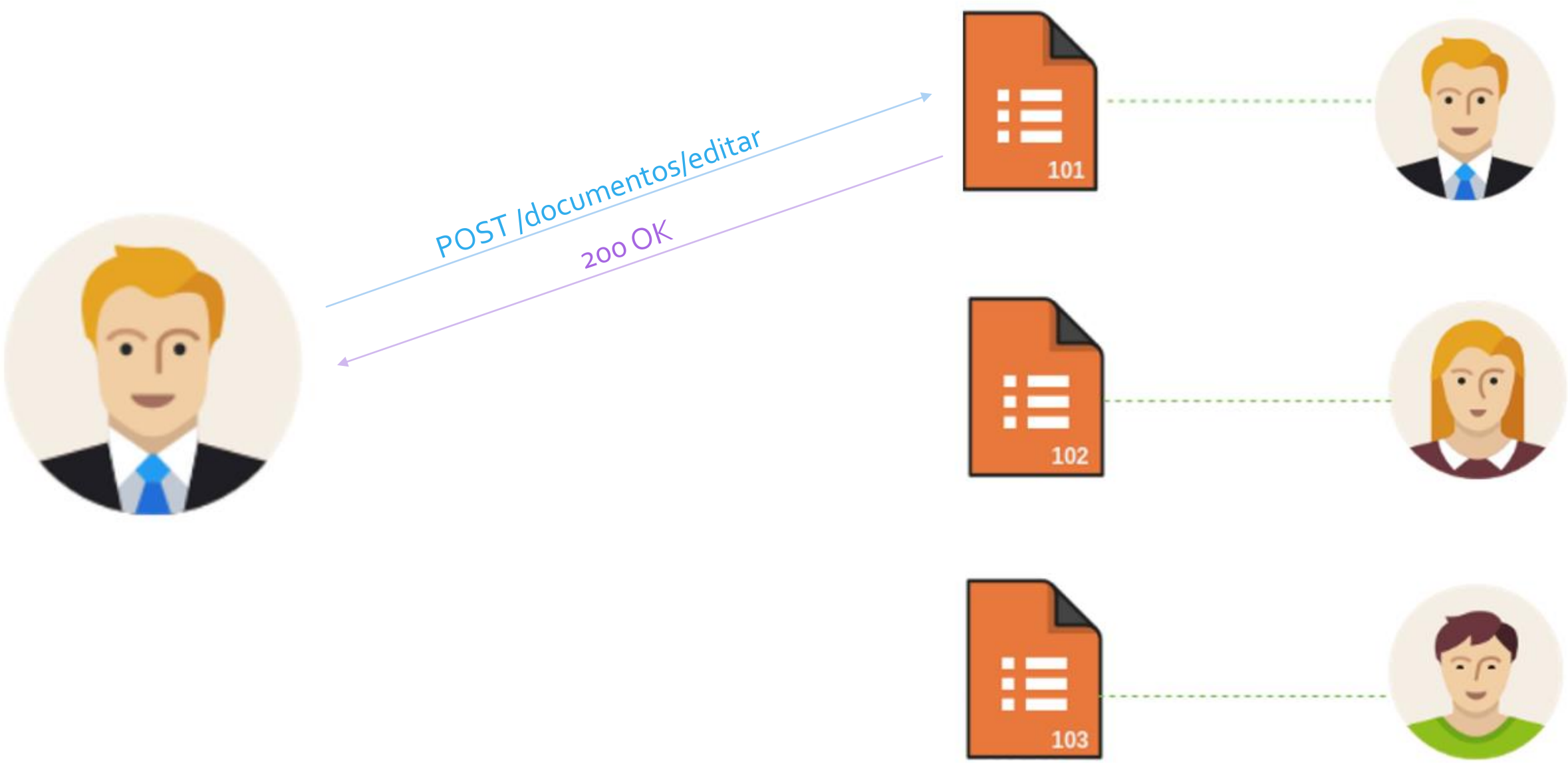

GET /documentos?id=101
200 OK
GET /documentos?id=103
200 OK
101
102
103

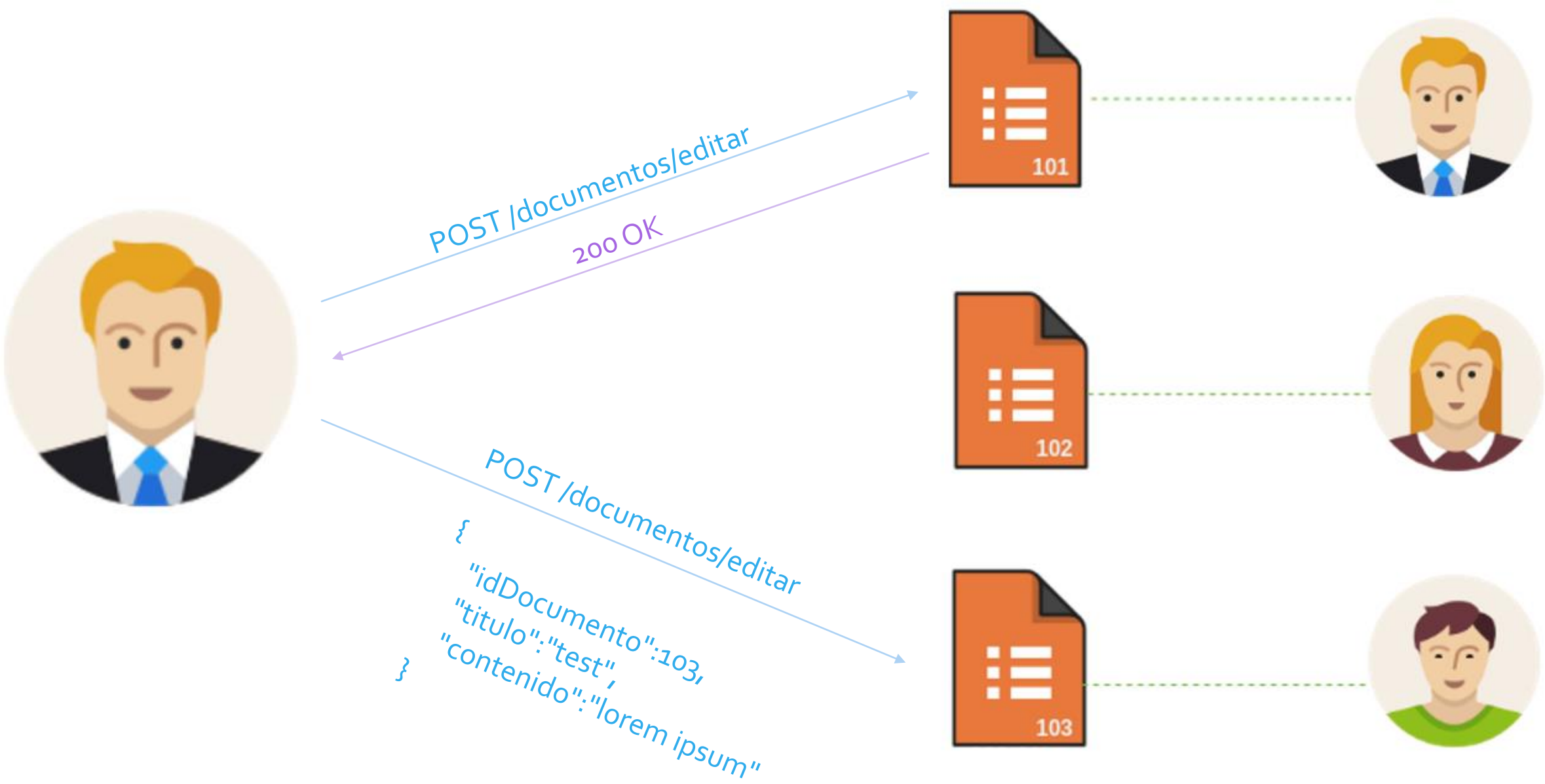

101

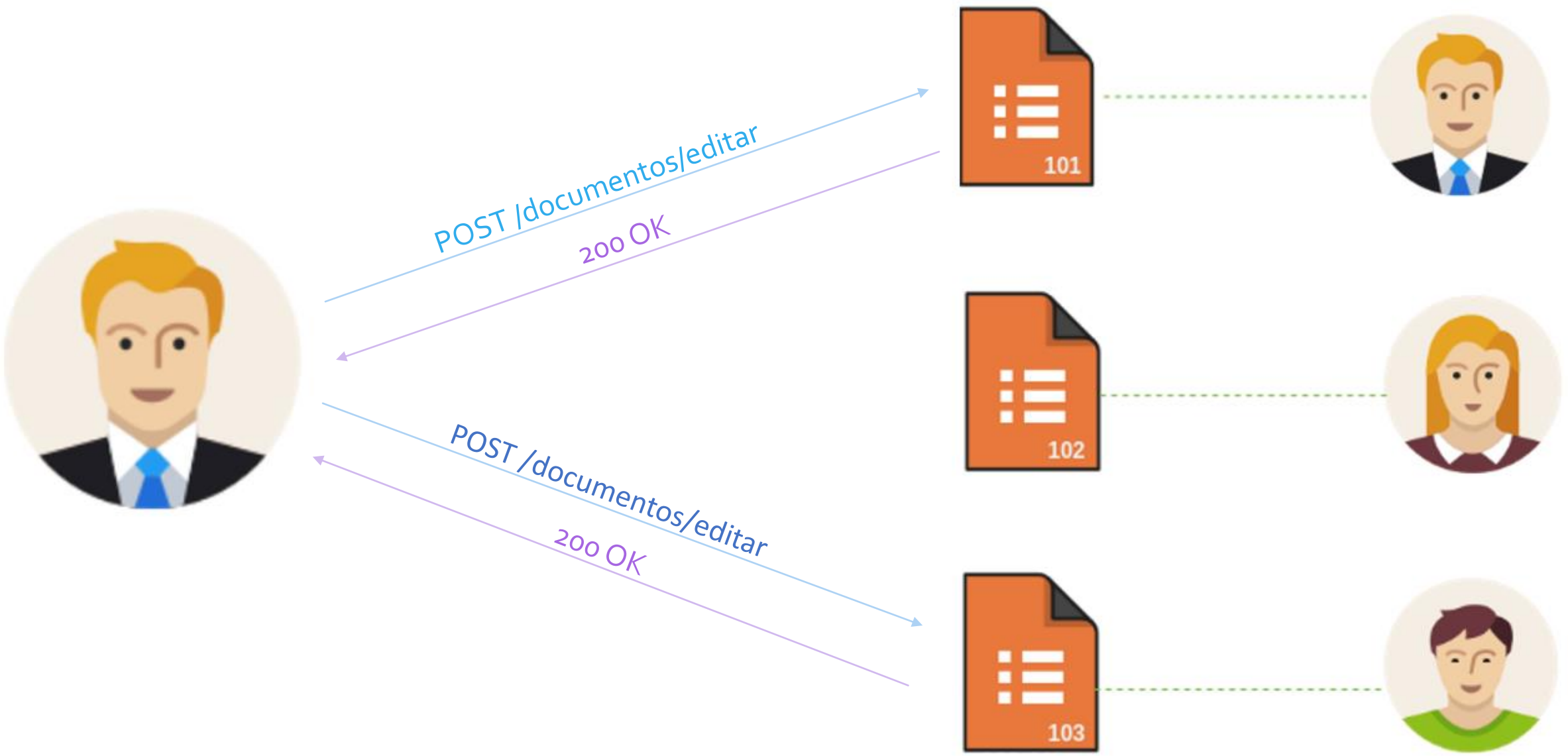

102


103


POST /documentos/editar
{
"idDocumento":101,
"titulo":"test",
"contenido":"lorem ipsum"
}
101
102
103


POST /documentos/editar
200 OK
101
102
103

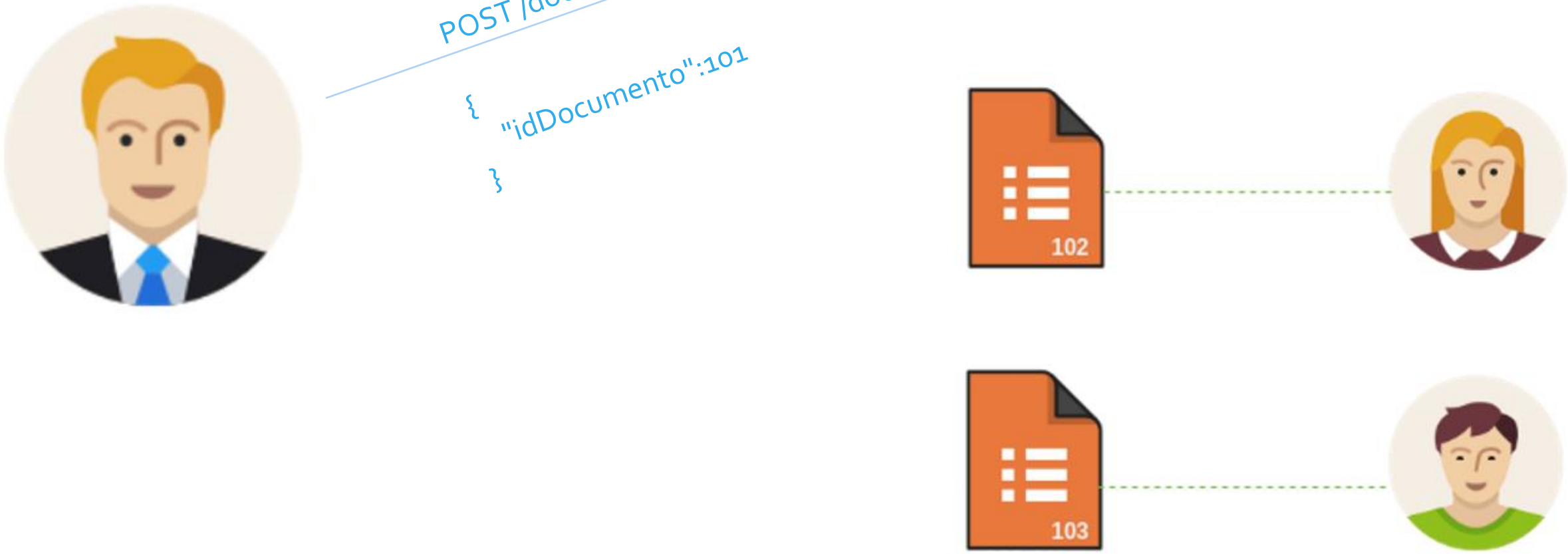

POST /documentos/editar
200 OK
POST /documentos/editar
{
"idDocumento":103,
"titulo":"test",
"contenido":"lorem ipsum"
}
101
102
103

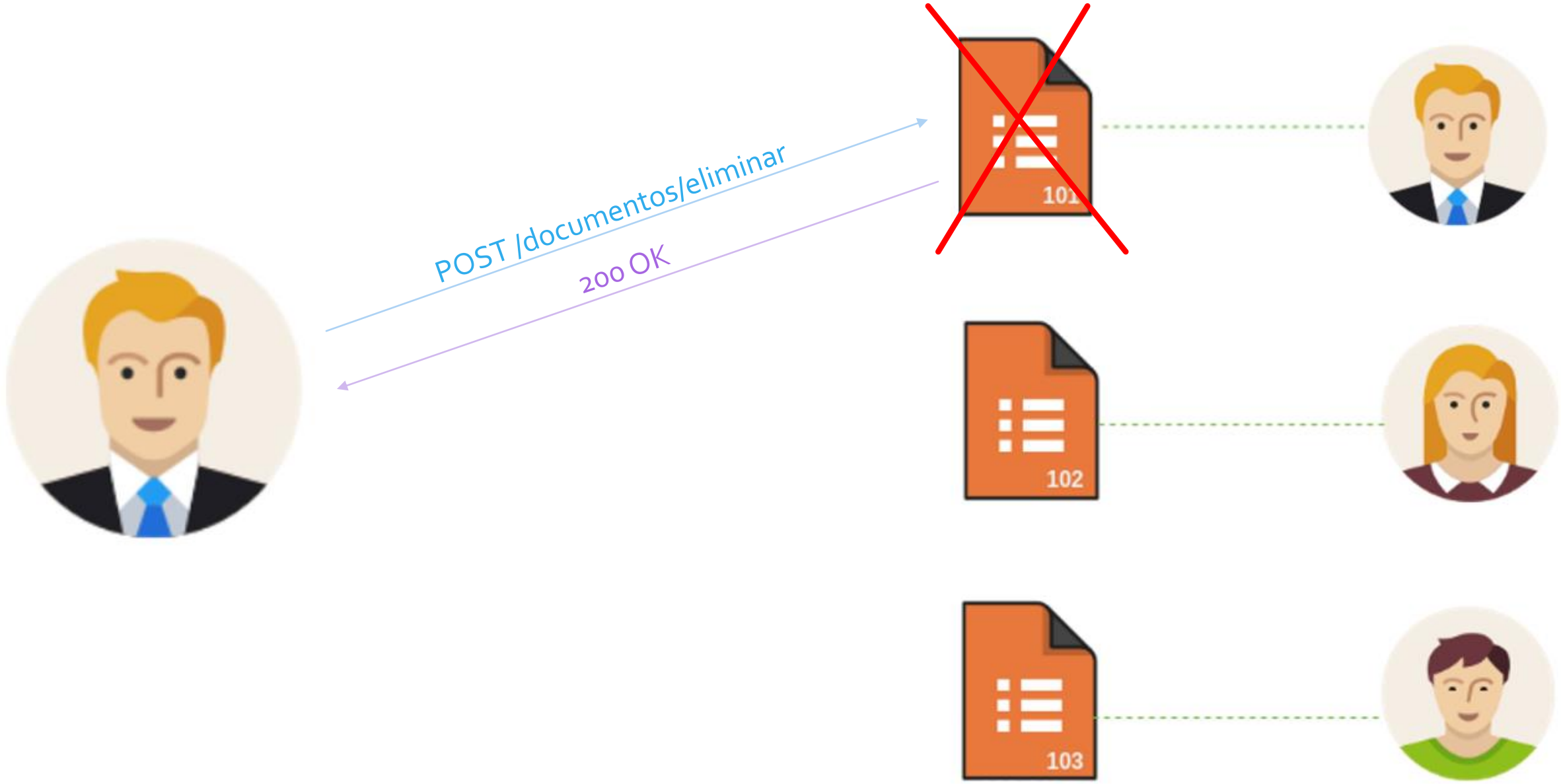

POST /documentos/editar
200 OK
POST /documentos/editar
200 OK
101
102
103

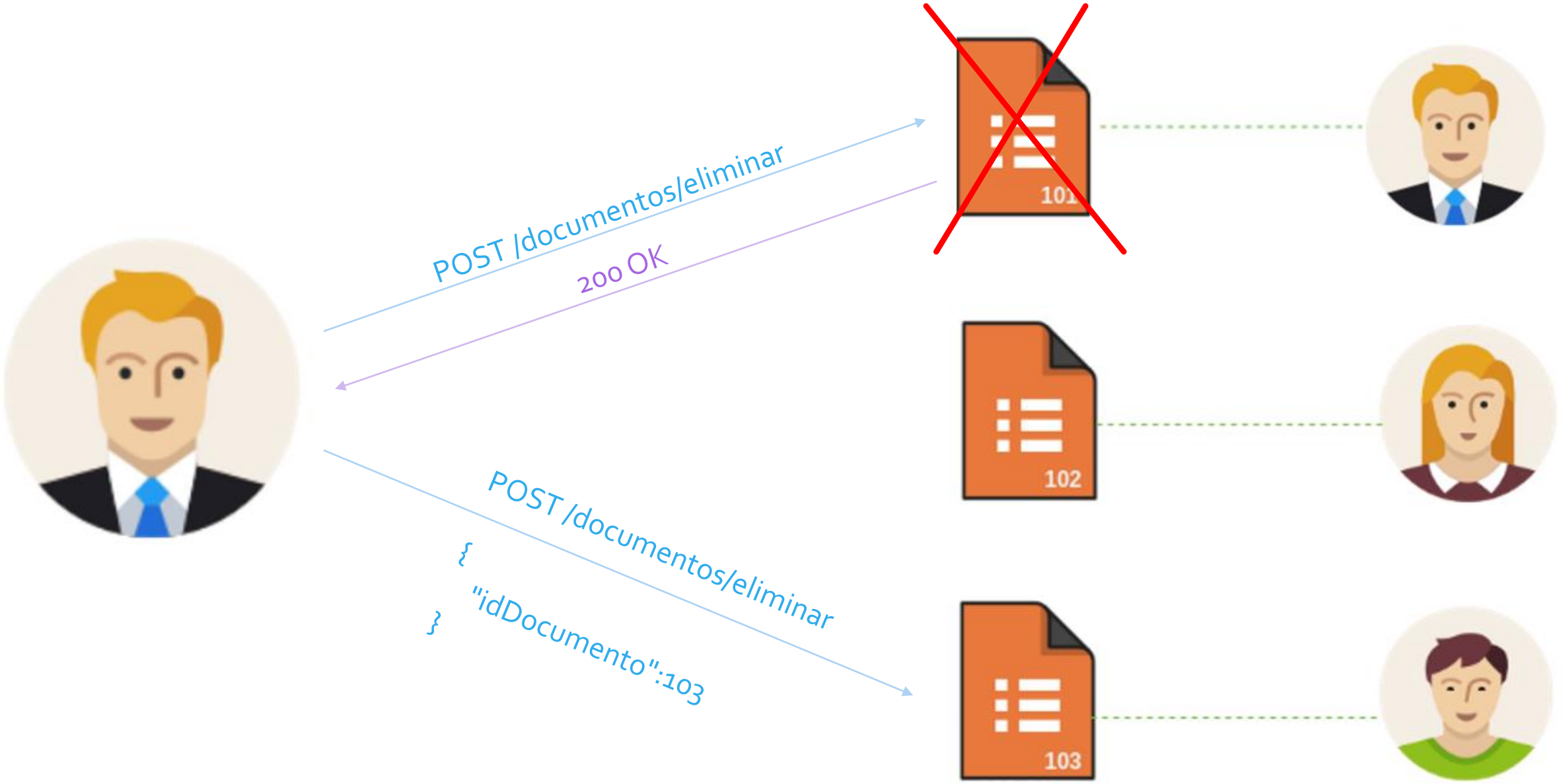

101

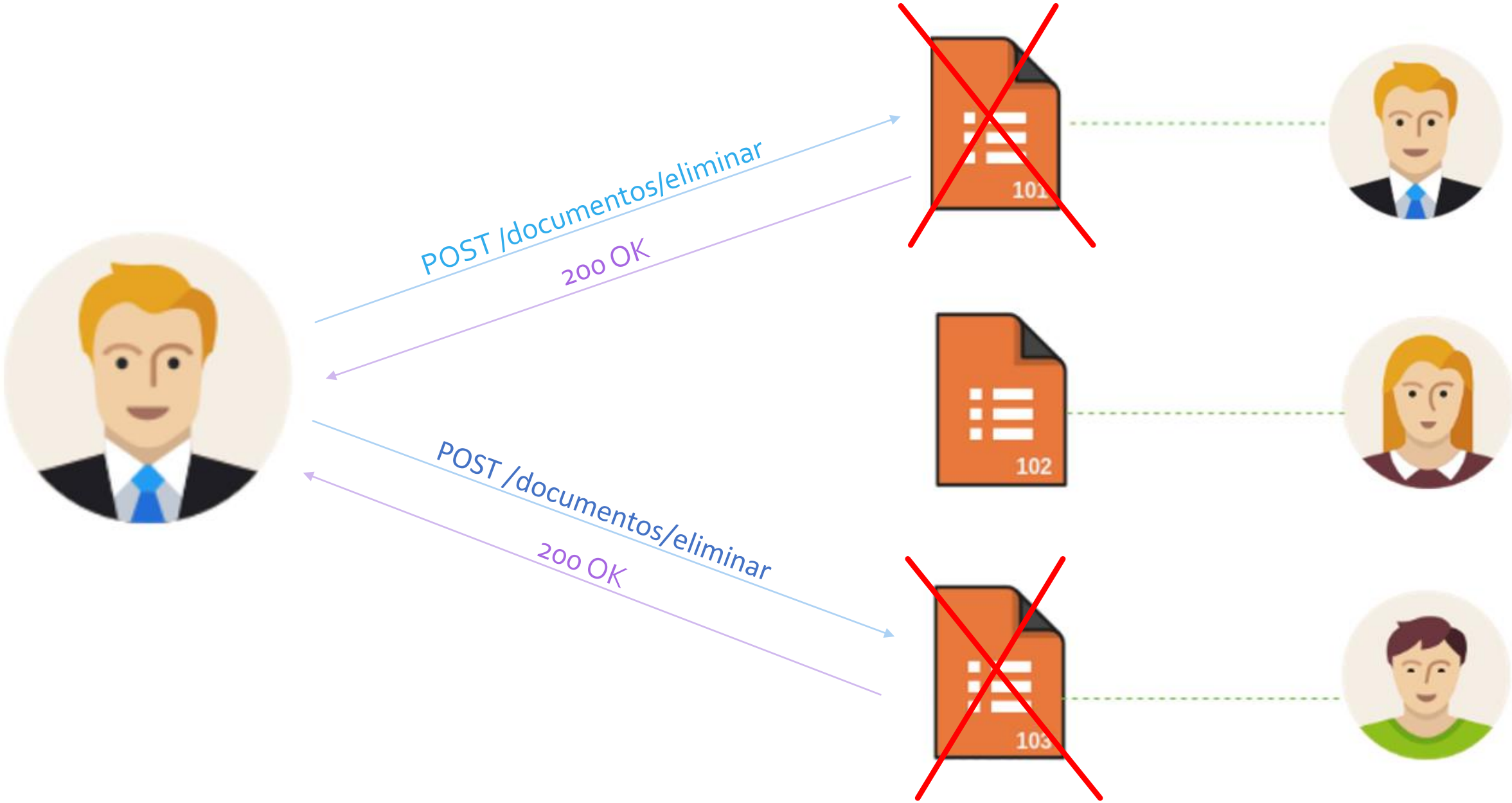

102


103

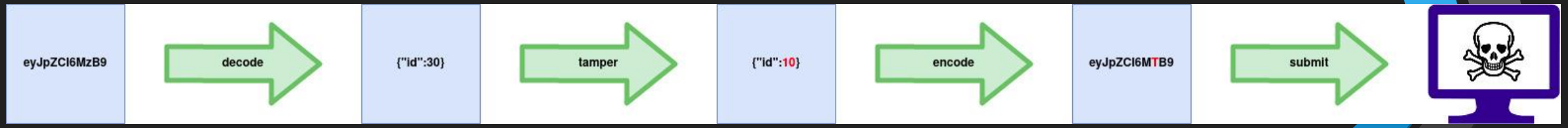

POST /documentos/eliminar
{
"idDocumento":101
}
101
102
103


POST /documentos/eliminar
200 OK
101
102
103


POST /documentos/eliminar
200 OK
POST /documentos/eliminar
{
"idDocumento":103
}
101
102
103


POST /documentos/eliminar
200 OK
POST /documentos/eliminar
200 OK
101
102
103

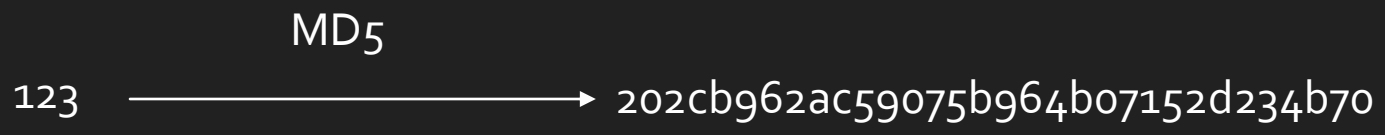
Encoded IDs



- Los desarrolladores web a menudo primero toman los datos sin procesar y los codifican.
- La codificación cambia los datos binarios a una cadena de caracteres, comúnmente utilizando a-z, A-Z, 0-9 y = para el relleno.
- La técnica de codificación más común en la web es la codificación base64 y, por lo general, puede ser bastante fácil de detectar.

Hashed IDs

- Las identificadores hash son un poco más complicadas de manejar que los codificados, pero pueden seguir un patrón predecible.



Ids impredecibes

- Si la identificación no se puede detectar utilizando los métodos anteriores, un excelente método de detección de IDOR es crear dos cuentas e intercambiar los números de identificación entre ellas.
- Si puede ver el contenido de otros usuarios usando su número de identificación mientras aún está conectado con una cuenta diferente (o no ha iniciado sesión en absoluto), ha encontrado una vulnerabilidad IDOR válida.

UUIDs/GUIDs

40d191c1-0aec-4815-af32-9f5374167b99

24fc52b0-d217-4f41-a35b-bfb9516a6c45