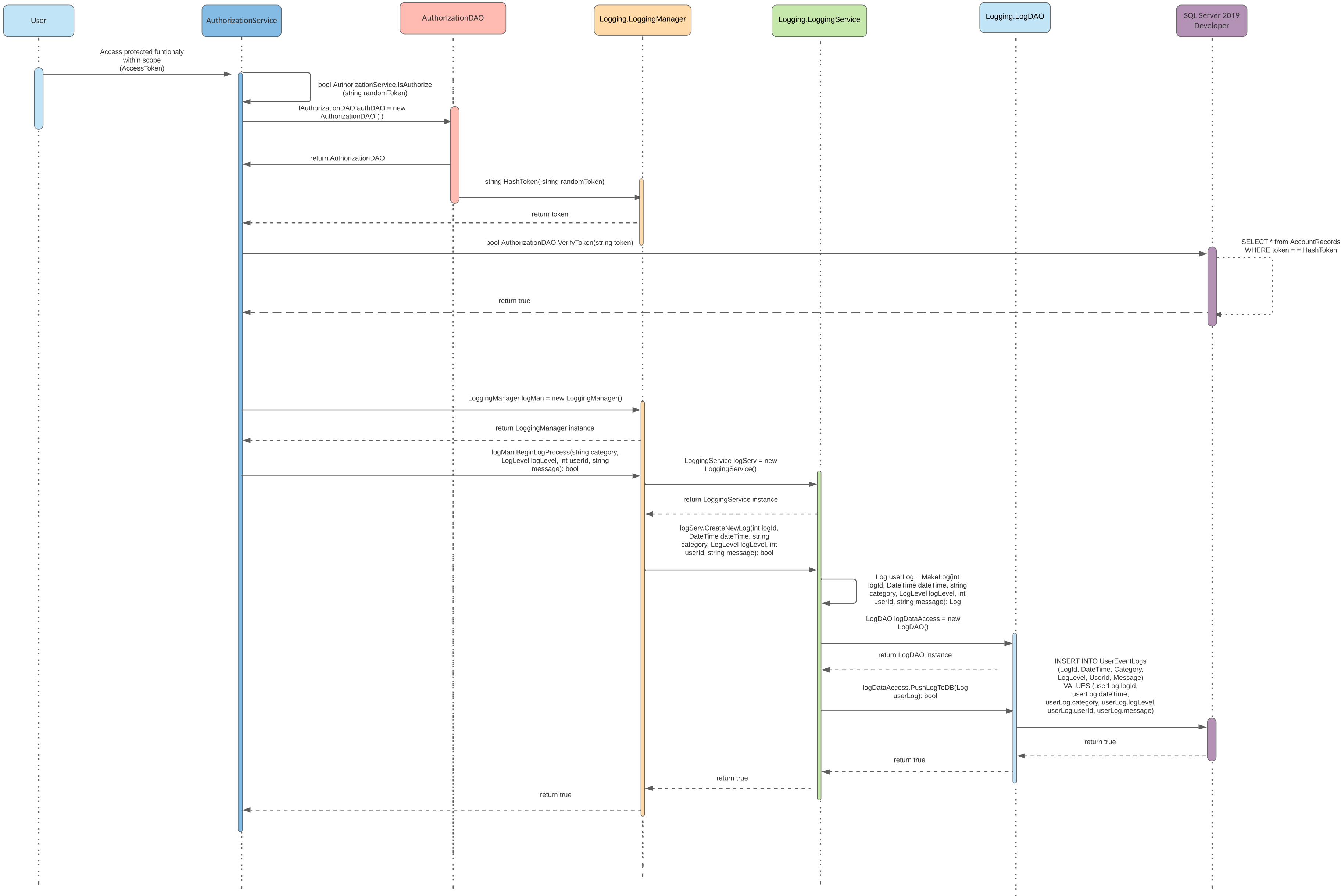
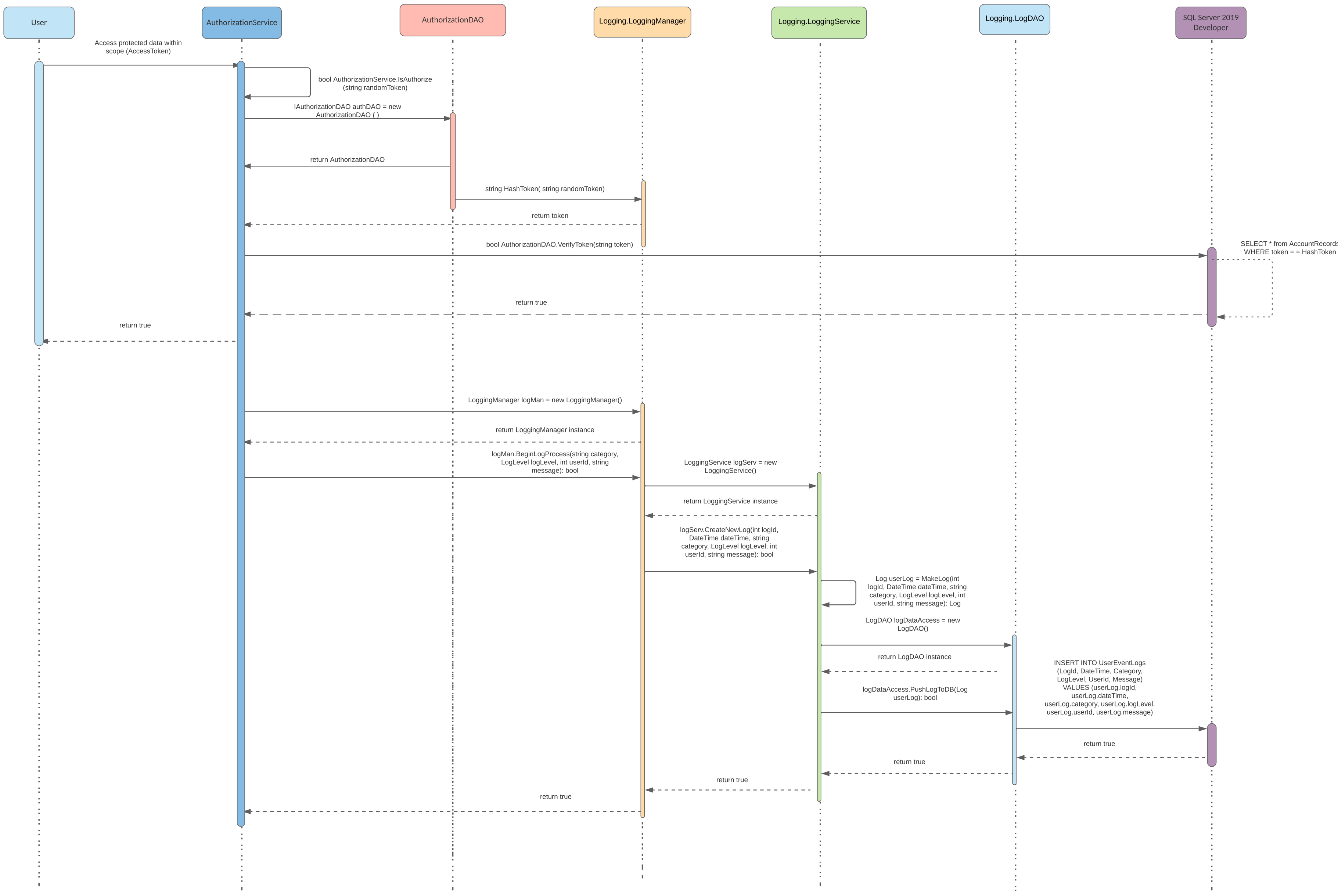


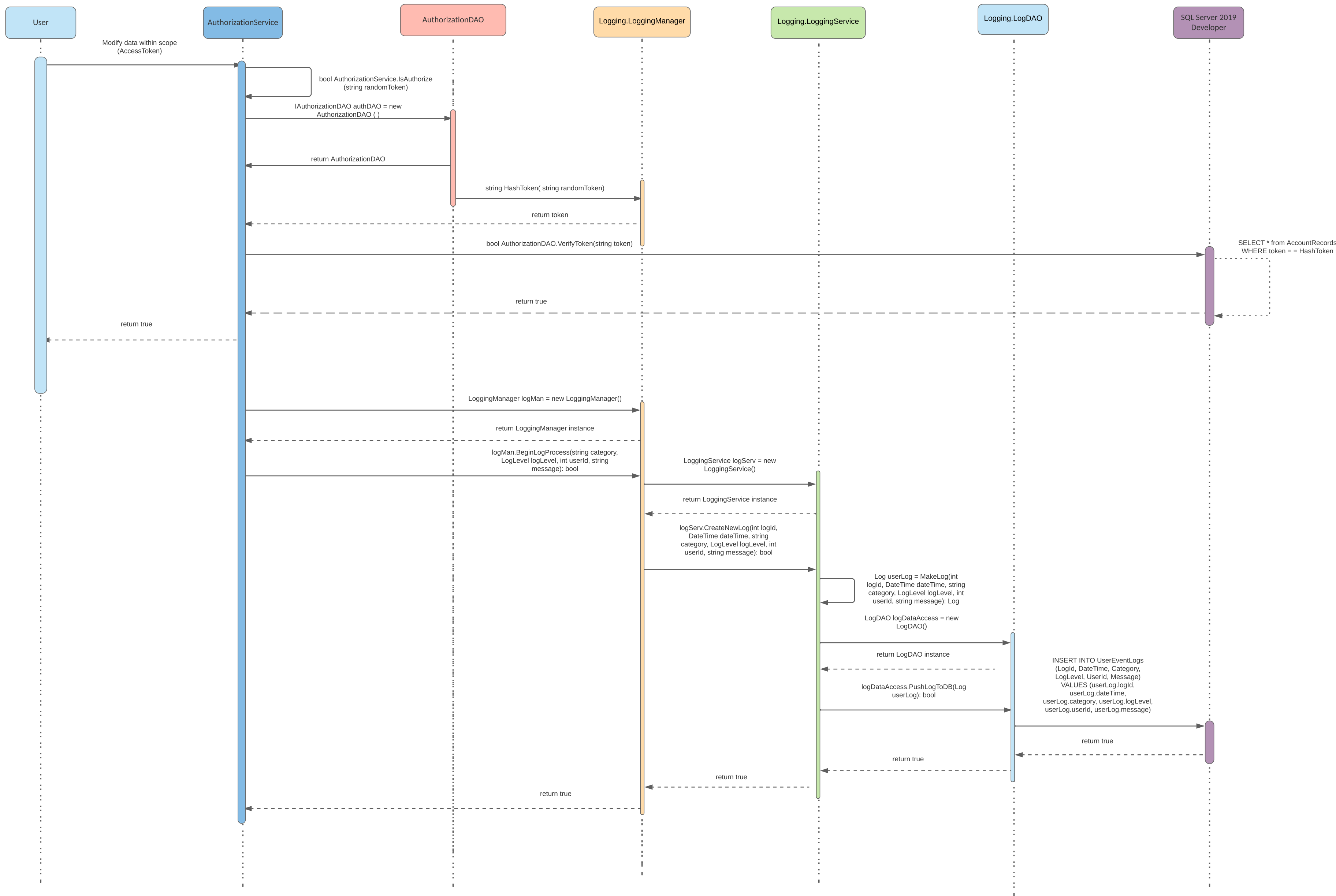
Success Case 1:
User attempts to access a
protected functionality within
authorization
scope. Access is granted to
perform functionality.



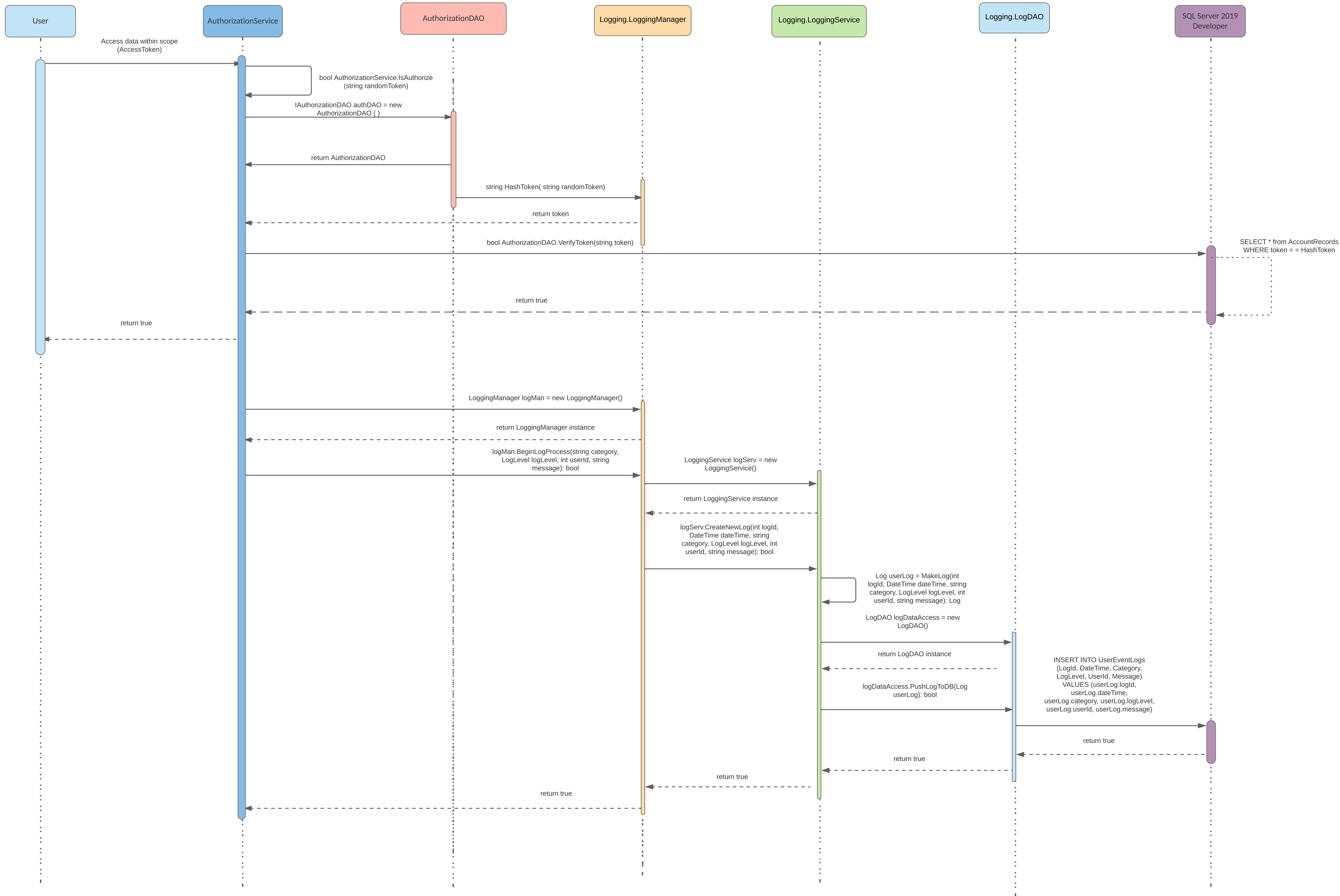
Success Case 2:
User attempts to access
protected data within
authorization scope. Access
is granted to perform read
operations.



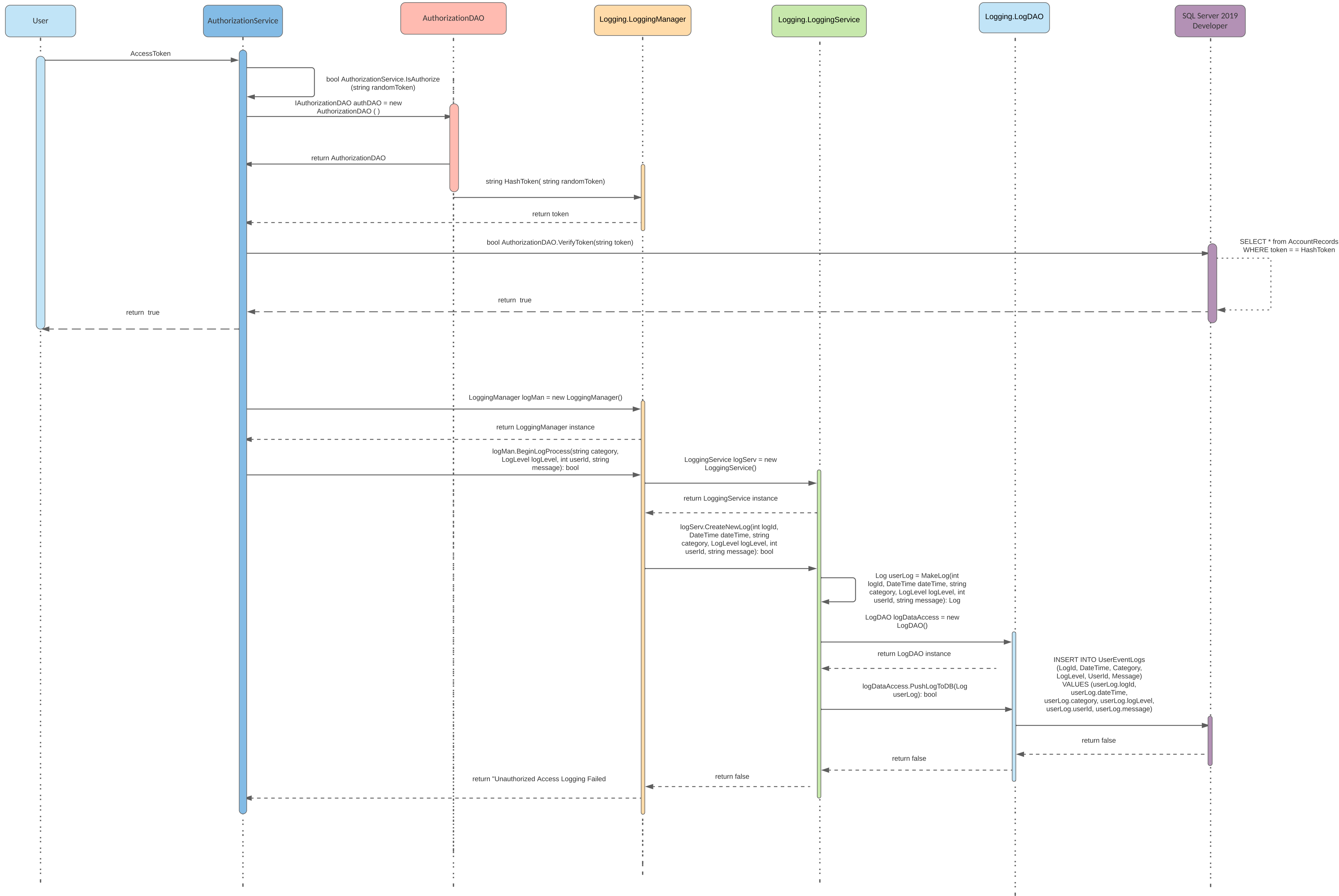
Success Case 3:
User attempts to modify
protected data within
authorization scope. Access
is granted to perform write
operations.



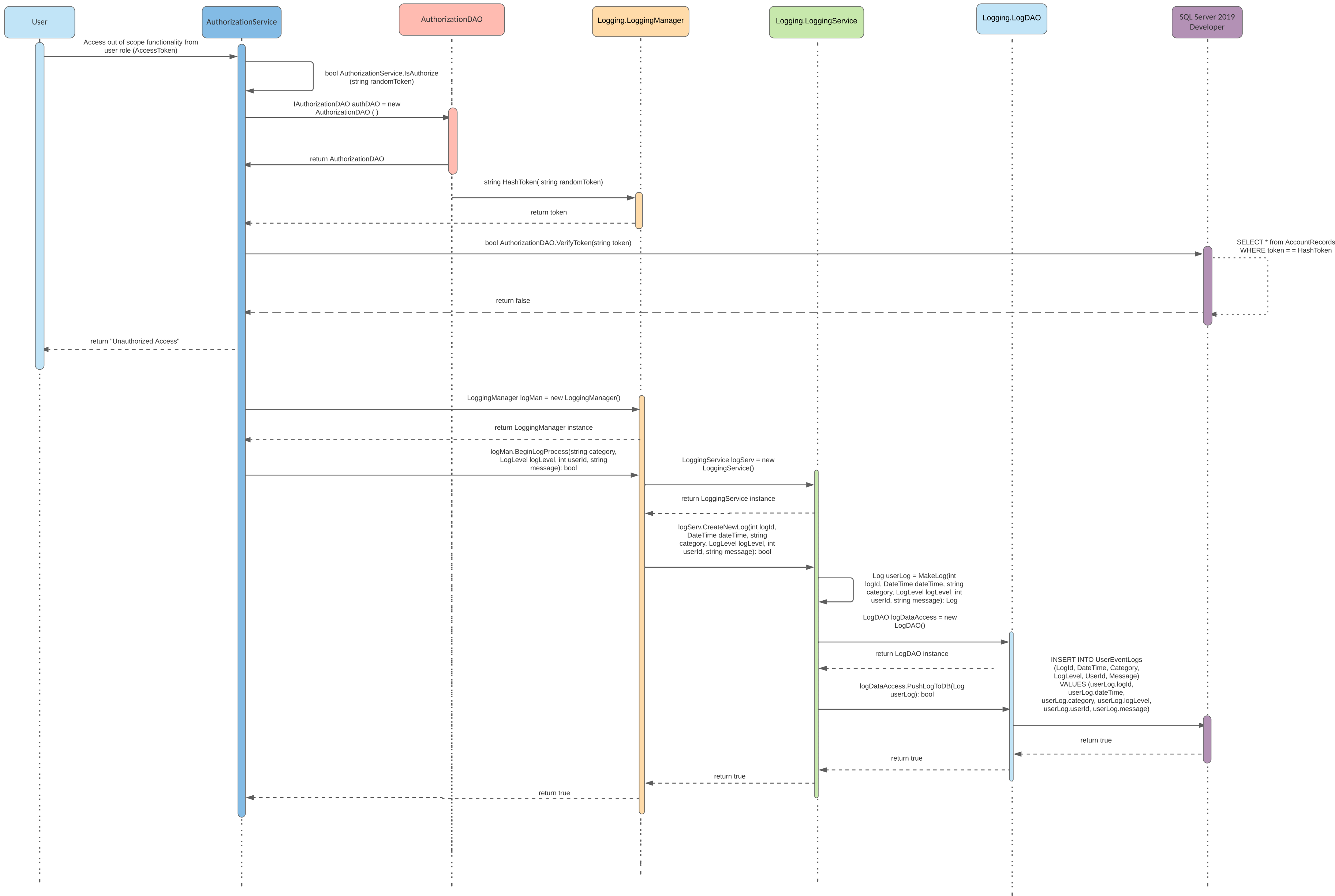
Success Case 4:
User attempts to access
protected views within
authorization scope.
Access is granted to the
view. User is automatically
navigated to view.



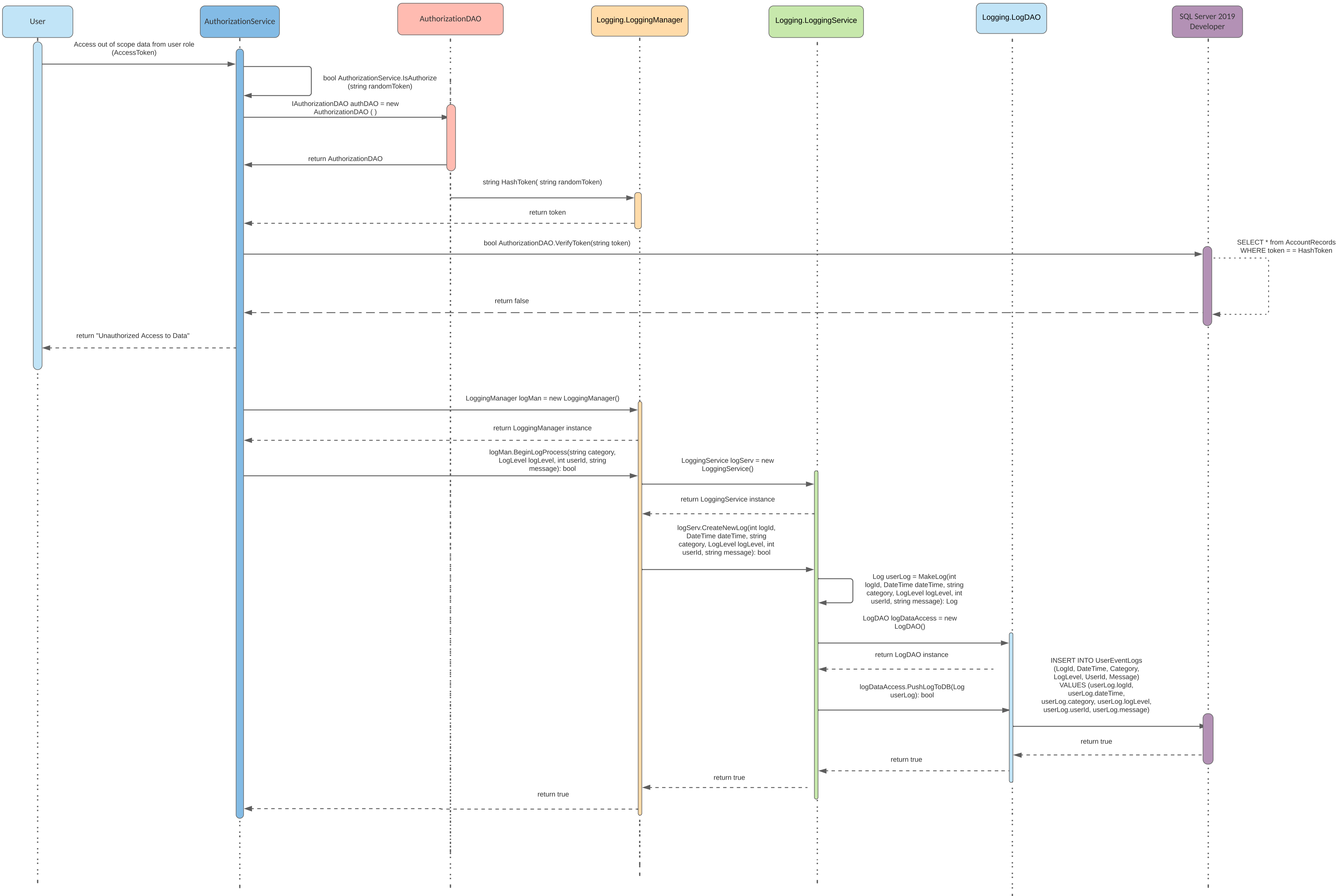
Failure Case 1:
Unauthorized access is not
recorded by system when
authorization fails. A system
log of failure is attempted.



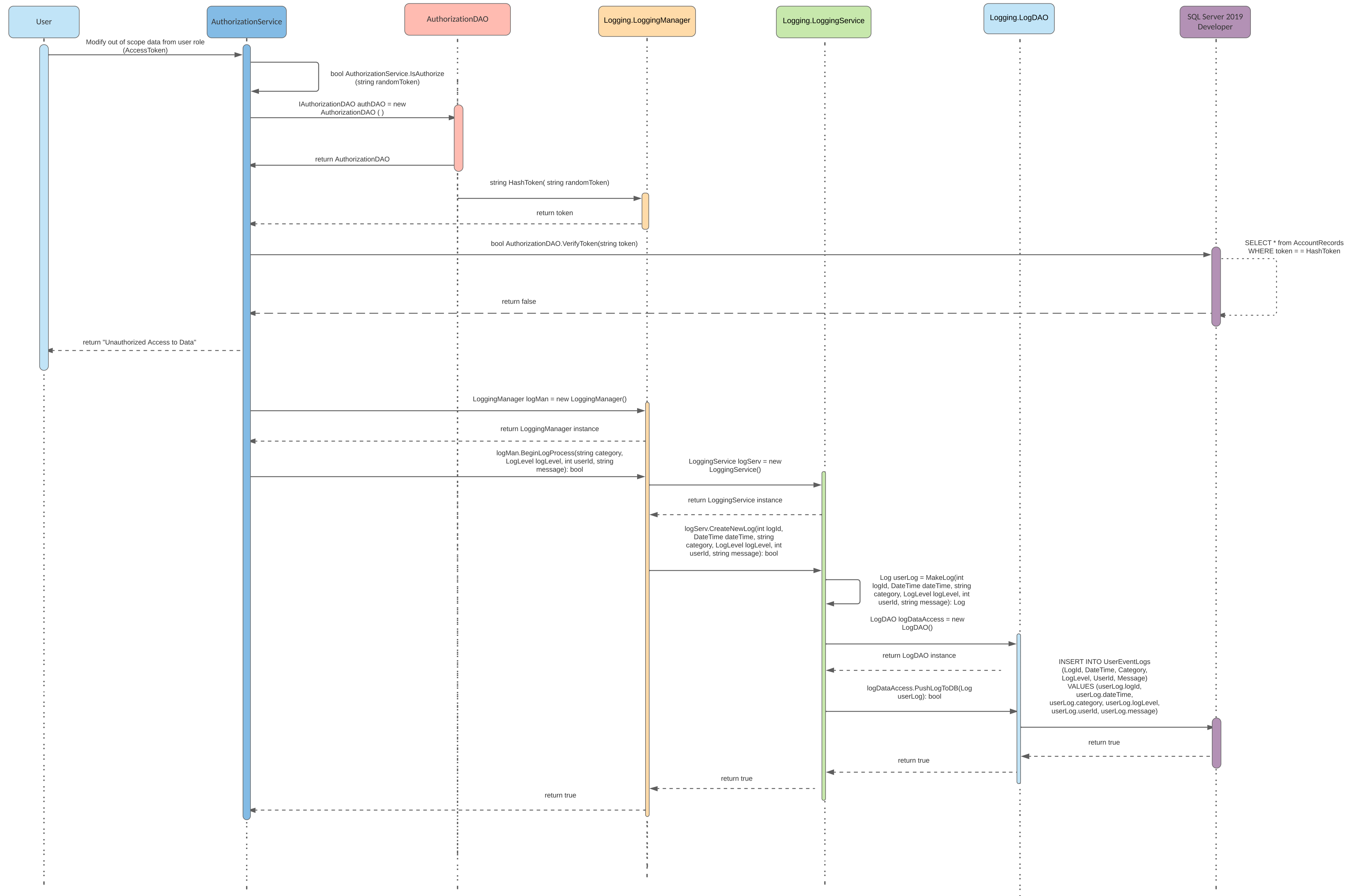
Failure Case 2:
User attempts to access a
protected functionality
outside of authorization
scope. Access is denied and
a system message displays
“Unauthorized access”.



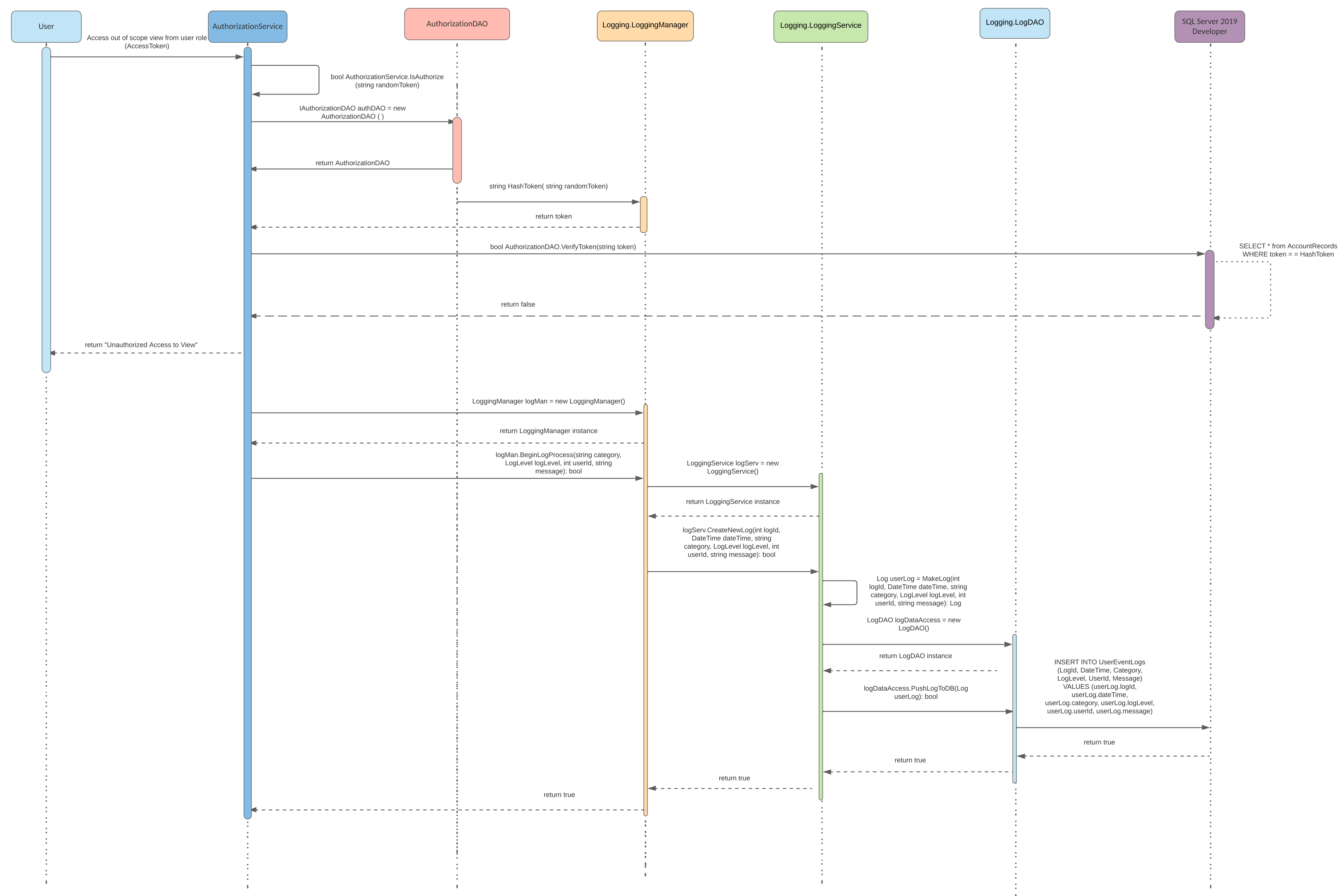
Failure Case 3:
User attempts to access
protected data outside of
authorization scope.
Access is denied and a
system message displays
"Unauthorized access to
data".



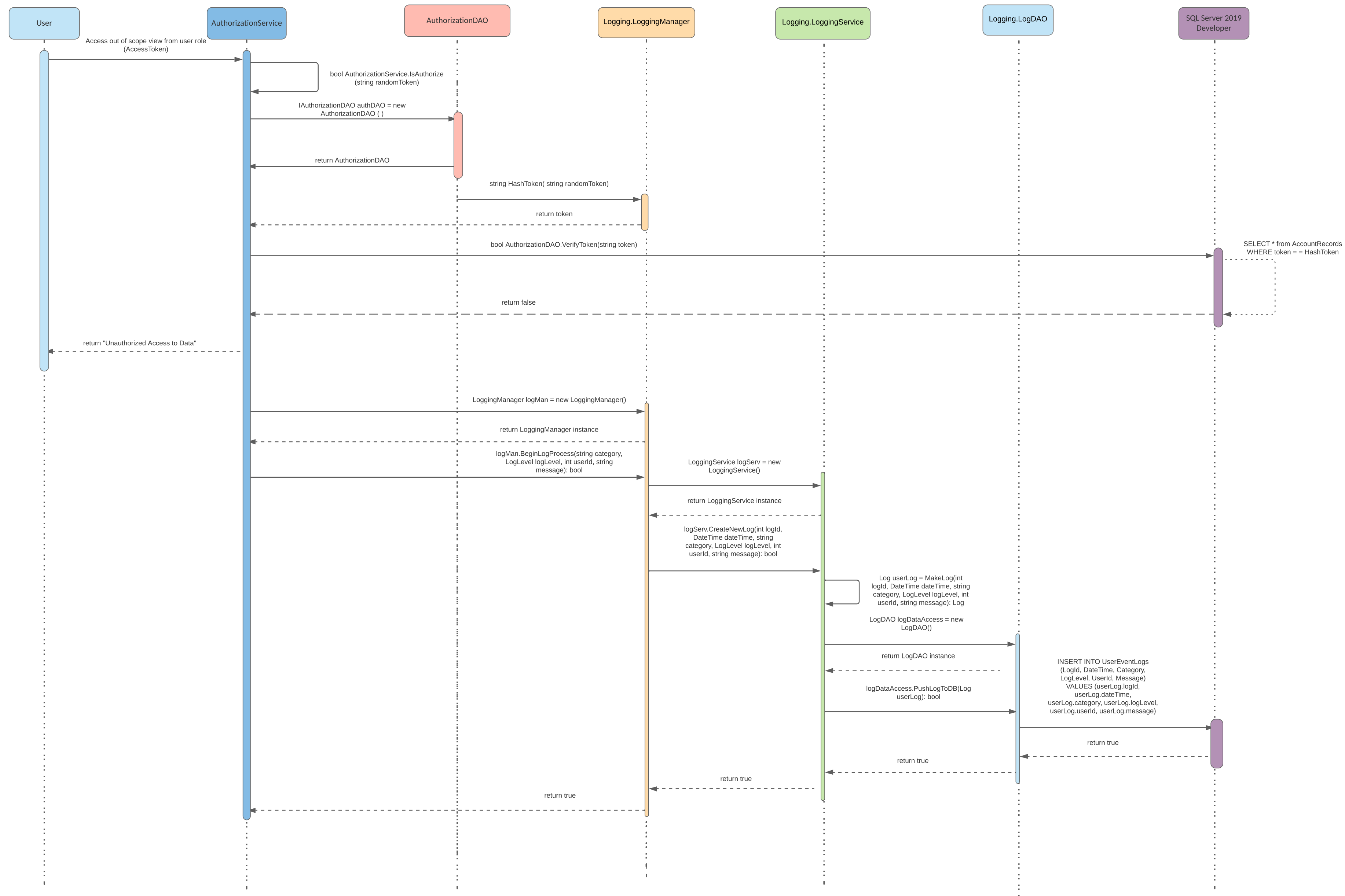
Failure Case 4:
User attempts to modify
protected data outside of
authorization scope.
Access is denied and a
system message displays
"Unauthorized access to
data".



Failure Case 5:
User attempts to access
protected views outside of
authorization scope.
Access is denied and a
system message displays
“Unauthorized access to
view”.



Failure Case 6:
User attempts to access
protected views within
authorization scope, but
contains protected data that
is not within read scope.
Access is granted to the
view. Upon
completion of automatic
navigation to view, a system
message displays
"Unauthorized access
to data" with protected data
not visible within the view.



Failure Case 7:
User attempts to access
protected views within
authorization scope, but
contains protected data that
is not within write scope.
Access is granted to the
view.
Upon completion of
automatic navigation to view,
protected data is visible
within the view.
Attempts to modify the data
will result in a system
message that displays
“Unauthorized
access to data”

