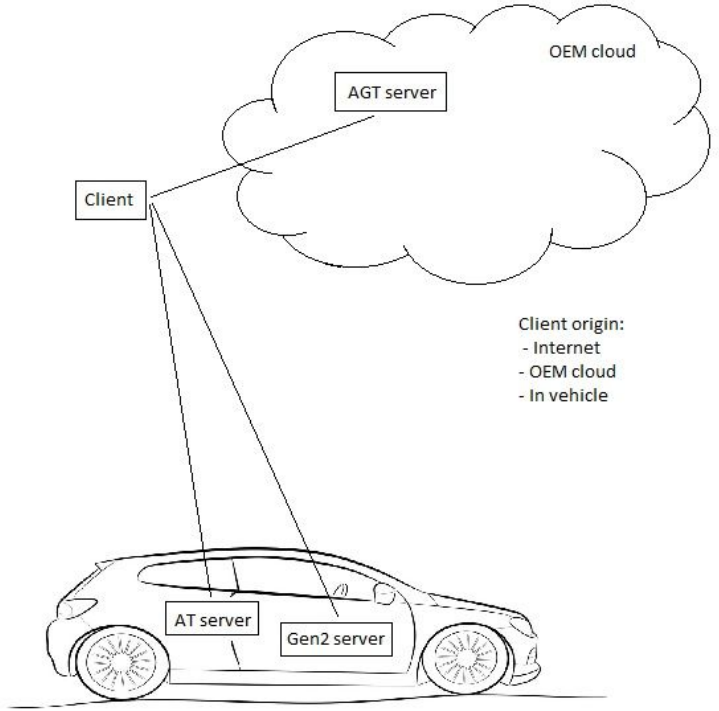
GEOTAB

W3C Gen2 access control model

Ulf Björkengren

W3C Gen2 access control overview

- Access control communication flow
  - Client - AGT server => Access Grant Token
  - Client - AT server => Access Token
  - Client - Gen2 server => Vehicle data



RBAC automotive modelling

```
Roles:

    -  Independent app, off-board
    -  OEM app, off-board
    -  Independent app, on-board
    -  OEM app, on-board
    -  OBD2 client
    -  Vehicle passenger
    -  Vehicle driver
    -  Vehicle owner
    -  Independent shop, remote access
    -  OEM shop, remote access
    -  Independent shop, proximity access
    -  OEM shop, proximity access
    -  OEM
```

Role-to-Permission table entry

```
    -  "RoleXPermission":
          -  "path": "path1", "access": "<read-only/read-write>"
          -  ...
          -  "path": "pathN", "access": "<read-only/read-write>"
```

- The table defines the maximum Permission scope for a Role. In the request to obtain AT token a subset of this, with associated purpose, is the typical scenario(?).

Communication flow details

1. Client requests Role to AGT server.
    - Input:
        - Client Id credentials for authentication
        - Requested role
        - VIN
    - Output:
        - AGT token:
            - Client Id
            - Role
            - VIN
            - Expiry time

2. Client requests IP access to vehicle. Off-board clients only.
    - Input:
        - AGT token
    - Output:
        - Vehicle URL
        - TLS credentials?

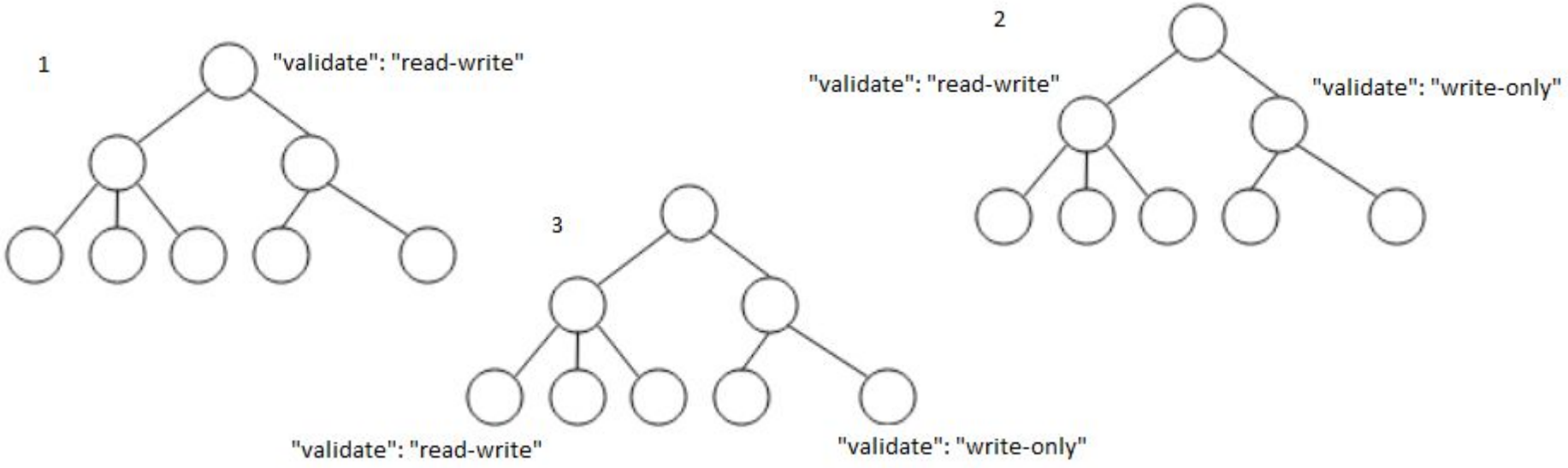
3. Client requests Permission to AT server.
    - Input:
        - AGT token
        - Requested permission
        - Purpose
    - Output:
        - AT token:
            - Client Id
            - Role
            - VIN
            - Permission
            - Purpose
            - Expiry time

4. Client requests data to Gen2 server.
    - Input:
        - Action
        - Path
        - AT token
    - Output: // After positive signature validation in request to AT server.
        - Value(s)

Design issues

- Why not only have one authorization server, the AGT server?
  - Client request typically require only subset of Role permission.
  - Permission shall be associated with Purpose.
  - Different expiry times on AGT and AT tokens.
  - Gen2 server shall not be required to communicate off-board for token validation.

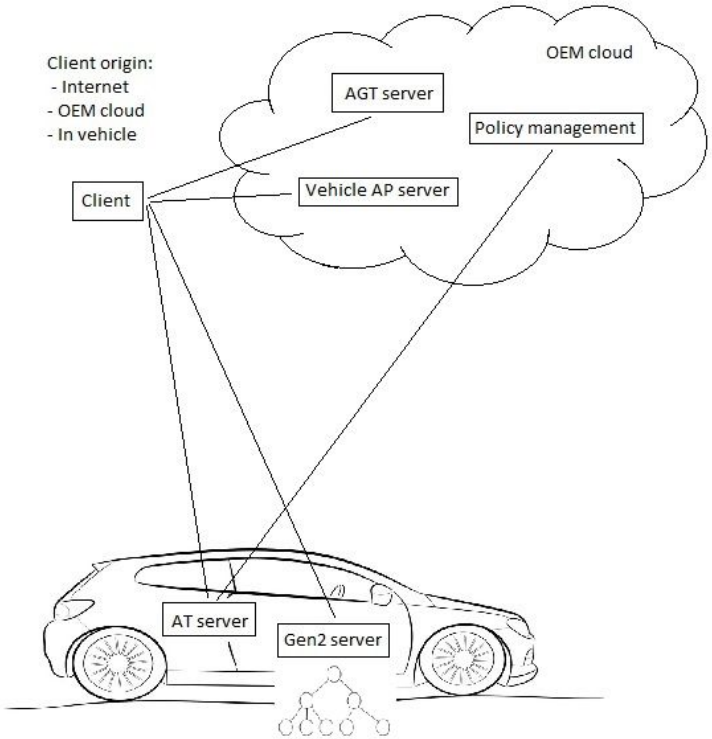
Access control tagging



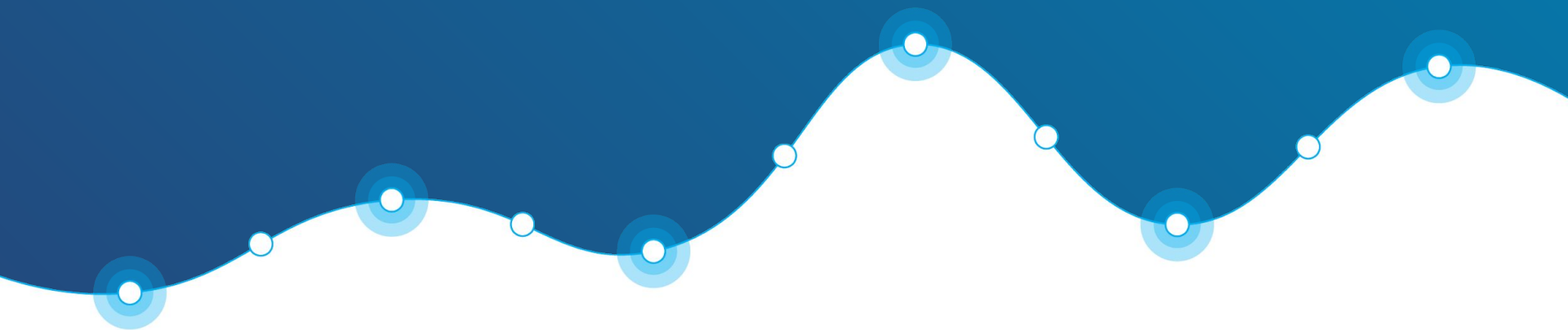
- 1: Complete tree requires valid token for both read and write requests
- 2: Two right-most leaves require valid token for write requests, the other leaves for both read and write requests.
- 3: Center leave nodes do not require any token for read/write requests, right-most require valid token for write requests, left-most for both read and write requests.

W3C Gen2 access control overview - complete

- A flexible access control model
  - No control / Write-only control / Read-write control
  - Role, Permission and Purpose modelling
    - RBAC type modelling
    - Privacy / Consent policy support
      - Can support a GDPR scenario?



Access control by default, or by design?



Arguments for access control by design

- Including tokens in a request increases request message size from about 100 chars to about 400 chars.
- On-board clients may be seen as more trusted, and hence may not require access control to all nodes.
- Client origin can be restricted to OEM cloud or on-board only, thus increasing their trustworthiness.
- Transport protocols shall always be secured, by e. g. running on top of TLS. A client must obtain communication credentials. And vehicle AP data.
- System development/debugging may be simplified by disabling access control.
- One line of metadata in the root node realizes default access control.

Do all of these VSS nodes require access control?

Vehicle.Body.BodyType

Vehicle.Body.RefuelPosition

Vehicle.Cabin.Door.Count

Vehicle.Cabin.Infotainment.HMI.CurrentLanguage:

Vehicle.Cabin.Infotainment.HMI.DateFormat:

Vehicle.Cabin.Infotainment.HMI.DayNightMode:

Vehicle.Cabin.Infotainment.HMI.DistanceUnit:

Vehicle.Cabin.Infotainment.HMI.EVEconomyUnits:

Vehicle.Cabin.Infotainment.HMI.FuelEconomyUnits:

Vehicle.Cabin.Infotainment.HMI.TemperatureUnit:

Vehicle.Cabin.Infotainment.HMI.TimeFormat

Vehicle.Cabin.Seat.DriverPosition

Vehicle.Cabin.Seat.RowCount

Vehicle.Chassis.Axle.Count

Vehicle.Chassis.Axle.RowX.TireDiameter:

Vehicle.Chassis.Axle.RowX.TireWidth:

Vehicle.Chassis.Axle.RowX.WheelCount:

Vehicle.Chassis.Axle.RowX.WheelDiameter:

Vehicle.Chassis.Axle.RowX.WheelWidth:

Vehicle.Chassis.CurbWeight:

Vehicle.Chassis.GrossWeight:

Vehicle.Chassis.Height:

Vehicle.Chassis.Length:

Vehicle.Chassis.TowWeight

Vehicle.Chassis.Wheelbase:

Vehicle.Chassis.Width:

Vehicle.Drivetrain.BatteryManagement.ChargingInlet

Vehicle.Drivetrain.FuelSystem.FuelType:

Vehicle.Drivetrain.FuelSystem.HybridType:

Vehicle.Drivetrain.FuelSystem.Range:

Vehicle.Drivetrain.FuelSystem.TankCapacity:

Vehicle.Drivetrain.InternalCombustionEngine.Configuration:

Vehicle.Drivetrain.InternalCombustionEngine.Displacement:

Vehicle.Drivetrain.InternalCombustionEngine.FuelType:

Vehicle.Drivetrain.Transmission.DriveType:

Vehicle.Drivetrain.Transmission.GearCount:

Vehicle.VehicleIdentification.Brand:

Vehicle.VehicleIdentification.Model:

Vehicle.VehicleIdentification.Year:

Vehicle.VehicleIdentification.bodyType:

Vehicle.VehicleIdentification.dateVehicleFirstRegistered:

Vehicle.VehicleIdentification.meetsEmissionStandard:

Vehicle.VehicleIdentification.productionDate:

Vehicle.VehicleIdentification.purchaseDate:

Vehicle.VehicleIdentification.vehicleConfiguration:

Vehicle.VehicleIdentification.vehicleModelDate:

Vehicle.VehicleIdentification.vehicleSeatingCapacity:

Vehicle.VehicleIdentification.vehicleSpecialUsage:

Vehicle.VehicleIdentification.vehicleinteriorColor:

Vehicle.VehicleIdentification.vehicleinteriorType:

Vehicle.accelerationTime:

Vehicle.cargoVolume:

Vehicle.emissionsCO2

Corporate headquarters:

Geotab Inc.
2440 Winston Park Drive
Oakville, Ontario
L6H 7V2, Canada

Tel: +1.416.434.4309
www.geotab.com

Geotab Waterloo

137 Glasgow Street,
Unit 340
Kitchener, Ontario
N2G 4X8, Canada

USA

770 E. Pilot Rd,
Suite A
Las Vegas, Nevada
89119, USA

Mexico City

Paseo de la Reforma 296
Juárez, 06600,
Mexico City, Mexico

UK

Geotab GmbH
3 Waterhouse Square
138 - 142 Holborn,
London, EC1N 2SW
United Kingdom

France

Geotab GmbH
67 Avenue de Wagram
Paris, 75017
France

Germany

Geotab GmbH,
Kaiserstr, 100
52134 Herzogenrath,
Germany

Spain

Geotab GmbH
Calle de la Princesa,
43 2ºD
28008 Madrid,
Spain

Italy

Geotab GmbH
Viale Citta d'Europa 39
00144, Rome,
Italy

China

Room 707, Mai Ke Long
Building, Science and
Technology Park, Nanshan
District, Shenzhen,
Guangdong, China 518057

Australia

Level 24 Westpac House,
91 King William Street
Adelaide SA 5000
Australia


Let’s Stay Connected:
@GEOTAB
GEOTAB
2440