RealityMobile

RealityVision® Mapping Engine: A Closer Look

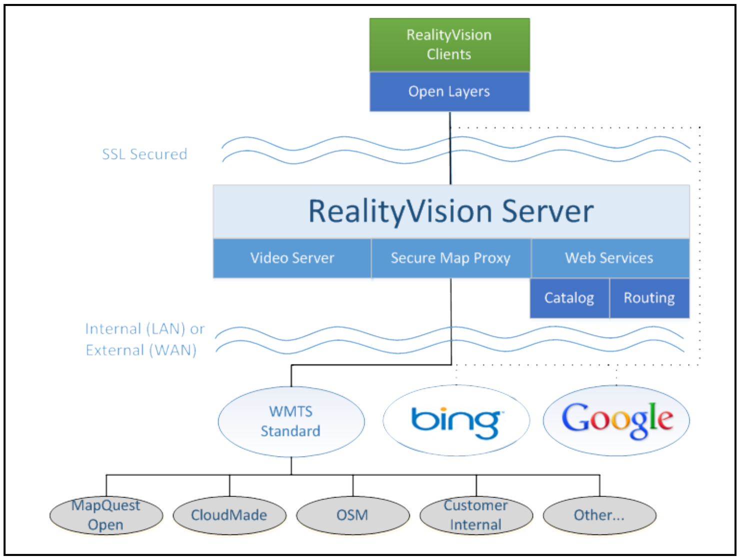
For years the RealityVision® platform has empowered mobile users to collaborate with each other in real-time in a highly visual way. User and camera locations have been displayed on Google, Bing or Apple maps to provide location context. Whether a user or a camera is near an incident, a workman is near a failed system, or a security officer or camera is near a tripped sensor, location provides a means of knowing who to contact or what camera to access when the need arises.

But what do you do when corporate assets are tracked on a private mapping server? Since earlier versions of RealityVision were tied to public mapping servers, this was not possible. What if the RealityVision system was run in a private network where cellular connectivity was not allowed? No access to public mapping servers was possible, so no location context could be shown. What if knowledge of what map regions are accessed needed to be kept private? Traffic to these servers could be monitored by technologically savvy competitors.

With RealityVision 3.4, Reality Mobile is introducing a new mapping engine that continues to allow the customer to rely on public mapping servers, but to alternatively secure that access inside their private network. This is accomplished by allowing customers to host private mapping servers that support the WMS, WMTS or Google APIs and to have the map tile requests hosted over SSL to keep the tile requests secure between the mobile edge and the RealityVision servers. With the new mapping engine customers can also add additional layers of asset information along side of the user and camera information already provided by RealityVision.

The Mapping Engine

RealityVision 3.4 introduces a new mapping engine to secure communications to the map tile servers in combination with OpenLayers to provide the mobile client map user experience. By using an open technology to provide the interactive map experience we have capitalized on years of development in geo-spatial technologies and provided an API for extension of the mapping technology that is well documented and familiar to those who have previously worked with mapping technologies.



The security layer is provided by routing the map tile requests through the RealityVision server, utilizing the same SSL security layer already in place for other RealityVision metadata and video footage. We have enhanced that layer by adding nonce (a single session random number) into the stream so that each user's requests for tiles have a unique signature, even when the same tiles are requested.

Unfortunately, Google and Bing Map tiles cannot be routed through our server since the addresses for their tile servers are embedded into their javascript API files. If a private Google Server is hosted in a private network, it is currently possible to adjust the tile requests inside the API files to route them through the RealityVision server. However, the method to access the tiles could change with future releases. Please contact us for more information if you have this configuration.

Private Map Server

The central extension to RealityVision is the capacity to allow customers to host their own map tile servers that contain custom mapping data central to their business and operations. The data embedded into these maps can be anything from oil fields to shipping routes. By hosting a WMS or WMTS tile server the mapping data is pre-rendered and cached for fast and efficient delivery to the mobile devices. No longer are Android devices tied to the Google Maps or iOS devices to the Apple maps. The source of mapping data is now up to the customer to decide.

Private Network Configuration

There are many situations where the system must be run completely in a closed network configuration: Ships at sea, facilities or factories with little or no cellular coverage, or simply for security considerations. In these environments access to public mapping servers are not just an issue, but impossible. With the ability to internally host a private map server, RealityVision can now provide map data to the mobile devices in any of these configurations through the use of WiFi networks, private LTE networks or any other private IP network configuration.

The Need for Tile Security

In some scenarios it is critical that map tile requests are not visible for public scrutiny. For some businesses just showing an interest in location information can expose their intent to competitors and weaken their competitive advantage. In blue force tracking scenarios it can expose to outside interests where key personnel or assets are located.

By securing requests for tiles this traffic can be hidden from prying eyes. Personnel can be tracked safely and securely knowing that their locations are not exposed through incidental traffic from their mobile devices.

Creating Custom Layers

This change is not just about security. It is also about extensibility. Adding custom asset information, incident locations or other live geo-location information on the map is not only possible, but relatively easy to accomplish. The RealityVision system provides a new extension point that allows for custom JavaScript access to the OpenLayers mapping API so that customer layers can be added at the server to be rendered on all RealityVision mobile clients.

Assets can be anything the customer has geo-location information for. For example, sensor location and status can be displayed by accessing the customer's own services and graphically representing that on the map either as icons or vector graphics. Incident regions tracked in another system that expose this data in the APIs can be requested and rendered as geo-regions for user visualization alongside their other assets. The limit to what can be displayed is limited only by the data available to the customer.