

D.DEPN.2.1	Cooperation architecture and requirements on content interfaces for interoperability
-------------------	---------------------------------------------------------------------------------------------

SubProject No.	SP 1.3	SubProject Title	DEPN
Workpackage No.	Topic 2	Workpackage Title	Openness & interoperability
Task No.	N.A.	Task Title	N.A.
Author(s)	Thijs de Graaff, Marcel Konijn, Paul van Koningsbrugge, Marco Annoni, Massimo Coccozza, Mats Rosenquist, Hans-Joachim Schade		
Dissemination level	PU		
File Name	DEL_DEPN_2.1_Interoperability_v1.1.doc		
Due date	1 February 2008		
Delivery date	1 February 2008		

Abstract	This document describes interoperability framework for the future world of cooperative systems
-----------------	------------------------------------------------------------------------------------------------

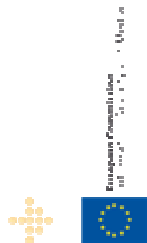
	<p>Project supported by European Union DG INFSO</p> <p>IST-2004-2.4.12 eSafety – Cooperative systems for road transport</p>
Project reference	FP6-2004-IST-4-027293-IP
IP Manager	Paul Kompfner, ERTICO – ITS Europe Tel: +32 2 400 0700, E-mail: cvis@mail.ertico.com

Table of Contents

TABLE OF CONTENTS	3
ABBREVIATIONS AND DEFINITIONS	4
EXECUTIVE SUMMARY	5
1. INTRODUCTION	6
2. OPENNESS AND INTEROPERABILITY	7
2.1. DEFINITIONS	7
2.1.1. <i>Openness</i>	7
2.1.2. <i>Interoperability</i>	8
2.2. APPLICABLE STANDARDS.....	8
2.3. RECOMMENDATIONS	8
2.4. REQUIREMENTS FOR CVIS APPLICATIONS	9
2.5. ABOUT THE USE OF SEMANTICS.....	9
3. COOPERATION ARCHITECTURE	11
3.1. PROBLEM AREA.....	11
3.2. SOLUTION DIRECTIONS	12
3.3. META DATA REGISTRATION	12
4. CONCLUSIONS	15

Abbreviations and Definitions

Abbreviation	Definition
ANSI	American National Standards Institute
API	Application Programming Interface
IEEE	Institute of Electrical and Electronics Engineers
CALM	Communication Access for Land Mobiles, provides a layered solution that enables continuous (or quasi continuous) communications between vehicles or between vehicles and the infrastructure. It is a ISO TC204 Working Group 16 standard
ISO	International Standards Organization
CVIS	Cooperative Vehicle Infrastructure Systems
DEPN	DEPLOYment eNabling, integrated project activity
ICT	Information and Communication Technology
ITS	Intelligent Transportation Services
ETSI	European Telecommunications Standards Institute
TC	Technical Committee
OASIS	Organization for the Advancement of Structured Information Standards
FOAM	Framework for Open Application Management (CVIS subproject)
GST	Global Systems for Telematics (EU project)
COMM	Communication and networking (CVIS subproject)
URI	universal resource identifier is a locator or a name of a resource or both. As a locator it provides means of acting upon or obtaining a representation of the resource by describing its primary access mechanism or network "location"

Executive Summary

The charter of Deployment Enablers Topic 2 is to devise a “cooperation architecture” for the exchange of information between applications included in the CVIS sub-projects. Also for all “content interfaces” requirements must be identified to ensure interoperability between the various system parts.

This document contains the interim opinion of the DEPN Topic 2 working group about the cooperation architecture and requirements for CVIS components with respect to interoperability. An update for this document is planned at the projects end.

The focus has been on deployment *after* the CVIS project, and less attention to the deployment of the CVIS example applications currently being developed, as these are likely to be replaced in the future by commercial software anyway.

The concepts ‘openness’ and ‘interoperability’ are defined like this working group feels they should be used within a CVIS context.

A few recommendations are given for development of CVIS applications and relevant standards are indicated, as well as specific requirements that hold for CVIS applications with implications for openness and interoperability. The meaning of semantics for the CVIS domain is treated briefly and consequences for design and implementation are indicated.

The cooperation architecture has to cope with various opportunities and threats that arise from trade offs that must be made. An enumeration of opportunities and threats is made that should be ticked off when taking decisions during trade offs.

For the short term, that is to say the period during which the CVIS project runs, the solution for openness and interoperability lays in the construction of a fixed CVIS data model, and appliance of a fixed set of well defined application interfaces and the framework offered by FOAM. For the long run, however, this approach will not provide a rigorous solution to an ever changing world. A more versatile solution is introduced by meta information describing the semantics of content exchanged.

The cooperation architecture for CVIS is based on various levels of interactions, comprising business models, business cases in the form of services offered, business protocols represented by contracts, service deployment and interconnection protocols.

The CVIS cooperation architecture is given as a CVIS “cooperation stack” of services and contracts together with more generic, supplementary standards and services like (open) standards, a semantic model sharing service and secure interoperability by proper identity services.

Finally, the conclusions summarize the most important implications of the work done in DEPN Topic 2.

1. Introduction

CVIS relevancy; its mission revisited

CVIS, cooperative vehicle infrastructure systems –more precise: vehicle-to-vehicle and vehicle-to-infrastructure systems– will allow vehicles to cooperate directly with other nearby vehicles, and with the immediate roadside infrastructure, thus sharing information on the latest road and traffic status for greater safety, efficiency and a better environment. Each equipped vehicle will be able to connect and communicate via local ad-hoc networks of vehicles and roadside equipment in the vicinity, and also via available mobile networks to access a wide range of journey support and other services.

The aim of CVIS is to develop an open and interoperable concept for cooperative systems, based on a standardized open architecture platform and common software modules for key applications: any equipped vehicle should be able to access and run any application, anywhere in Europe where there is compatible roadside infrastructure, mobile networks or nearby vehicles.

CVIS DEPN Topic 2 charter

The goals of the horizontal Deployment Enablers activity are in general to:

- Ensure that the core technologies and applications as developed in the CVIS project are fundamentally deployable and that non-technical issues have been identified and their potential impact on deployment described along with recommendations as to how these issues could be addressed;
- Derive road maps on how to migrate from today's situation, via an intermediate phase when penetration of equipped vehicles and infrastructure grows to a critical mass, to a future with widespread take-up of operational CVIS, based on transparent deployment and cooperative business models with suitable sharing of responsibilities and liabilities;

and, more detailed, Topic 2 has the goal to:

- Devise a “cooperation architecture” for the exchange of information content between all entities involved in the set of applications included in the CVIS sub-projects;
- For all “content interfaces” between entities, identify the requirements to ensure interoperability between systems.

About this document

This document contains the interim opinion of the DEPN Topic 2 working group about the cooperation architecture and requirements with respect to interoperability. An update will follow at the projects end.

Also there has been a focus on deployment *after* the CVIS project, and less attention to the deployment of the CVIS example applications, as these are likely to be replaced in the future by commercial software.

2. Openness and Interoperability

2.1. Definitions

Hereafter we will define the concepts ‘openness’ and ‘interoperability’ as we feel they should be used within a CVIS context. We will not give a definition straight away, but rather touch upon aspects that describe the concepts or, in contrary, that are excluded from the concepts.

2.1.1. Openness

For the meaning of “openness” we have to think about the nature of cooperative systems. Cooperative systems should be ‘open’ in such a way that:

inclusion	exclusion (i.e.: ‘openness’ is <u>not</u>)
<p>Each actor, be he private or public, should be able to plug his service into this environment</p> <p>It should be possible to make use of each other (sub) services.</p> <p>The services should be able to be distributed freely</p> <p>It should be possible to exchange information with each other for particular services. The type and nature of information exchange can differ per service. For instance the systems of the public road authorities will be open such that applications can read and write back. However it will not be completely open. There will always be security aspects to prevent systems from being hacked.</p> <p>It should be relatively easy to develop new services for the CVIS environment. No extensive knowledge of the other systems is required.</p> <p>Using established public standards related to the CVIS environment and available de-facto ICT standards, for software and communication.</p> <p>It has well documented interfaces</p>	<p>A vendor lock in of a specific system</p> <p>An environment which is to be developed with special tools</p> <p>A black box which can not be communicated with from outside</p> <p>Containing indispensable interfaces and system components “hidden” within a proprietary “black-box” and at the same time requiring the use of this sub-system.</p> <p>A service which is solely based on a specific communication technology that might be banned by some national or local regulation</p>

2.1.2. Interoperability

Also here we have to think about the nature of cooperative systems. Cooperative systems should be ‘interoperable’ in such a way that:

inclusion	exclusion (i.e.: ‘interoperable’ is <u>not</u>)
<p>A new service build in accordance with CVIS principles and recommendations can communicate with the environment and perform as expected</p> <p>Can run on various hardware platforms</p> <p>A CVIS service will behave independently of the involved actors and sub-system suppliers.</p> <p>Vehicles moving on the road infrastructure are able to use ITS services from different service providers, whenever presented to the users in the consistent and uniformed way of the CVIS recommendations</p>	<p>A service will only perform as expected in a specific environment</p> <p>When CVIS enabled vehicles using the road infrastructure are not able to use available ITS services</p> <p>Specific ITS services behaving differently depending on the service providers and the client systems involved</p> <p>When vehicles roaming in different countries cannot be provided with a local service “equivalent” to the one subscribed to or provided in its home country</p>

2.2. *Applicable standards*

Beside the general standards as issued by bodies like ANSI and IEEE also standards like emerging from the open source initiatives are relevant, the CALM ISO standard and the ETSI TC ITS.

Current open standards can be found at the website¹ from OASIS (Organization for the Advancement of Structured Information Standards), and for identity assurance through the website² of the Liberty Alliance.

Within CVIS the application framework offered by the FOAM subproject (Framework for Open Application Management, which amongst others heavily relies on the work done by GST project) is highly recommended as the way to develop, distribute and deploy CVIS services.

2.3. *Recommendations*

For development of CVIS applications it is recommended that one:

- adheres strictly to the CVIS recommended practices for application design (like f.i. as laid down in CVIS deliverables D.FOAM.3.1, D.COMM.3.1, and D.COMO.3.1)
- builds whenever possible on the CVIS Framework for Open Application Management
- is aware during the design phase of possible vulnerabilities to compromising the

¹ <http://www.oasis-open.org>

² <http://www.projectliberty.org>

systems integrity and builds in proactive counter measures (like for instance identity assurance and also critical performance issues)

- adheres to general standards for application development as available from ANSI and IEEE.

2.4. Requirements for CVIS applications

CVIS applications are meant to co-exist and to co-operate without any adverse interference. However, the context within which the applications practically will run cannot be predicted accurately. There will be a kind of local and global context to take into account. The (highly volatile) local context comprises temporary present objects in the vicinity of the applications user, whereas the (more statically in space and time) global context touches upon the global infrastructural elements of the CVIS world (e.g. back office systems, standard services, et cetera).

As the CVIS system relies heavily on resources with a limited capacity in for instance bandwidth, computing performance, availability, et cetera, it exhibits the nature of real time systems and the corresponding challenges.

Another aspect of the CVIS system is the continuous change in services offered to the end user, as well as the deployment of software upgrades and updates, maintaining equivalency of services over larger areas, compatibility of information, et cetera.

Bearing the previous in mind the following requirements hold for CVIS applications:

- It should be possible to develop and deploy applications forming services based on available system components even if the system is not complete. Then the applications forming the building blocks for a service should be possible to independently be replaced, updated and enhanced when the service is maturing.
- An application should at large be independent from others giving the possibility to independently replace it.
- The issue of “co-operation” among different concurrent applications should be taken into account during developments. Up to now in the CVIS project all applications have been conceived as stand-alone processes without taking care of any co-ordination with the other applications and with full use of all the processing and communication resources. In a real deployment this might cause the provision of conflicting or wrong information. Moreover, when the application requires an interaction with a human being, the human factor should be carefully considered in order to avoid the provision of too much information (or conflicting information) that may be a distracting factor and decrease the driver safety.
- It is highly recommendable to devise a resource sharing mechanism on a CVIS base level (in the CVIS cooperation stack; see also section 3.2) in order to budget the resource use per application. Likewise, for human interaction budgets should be defined per application given the set of applications active at any time. Applications must be budget aware in the above respects.

2.5. About the use of semantics

The use of a semantic approach is highly desirable given the diversity of the ITS world and the long time range for which the CVIS system is to be designed. The required supportive



means to provide for a proper interoperability for CVIS applications is still not in place to date. The best attempt known is the initiative taken by the UK Highway Authorities running a pilot project on their ITS Metadata Registry.

At this time it can be foreseen that convergence of ITS information descriptions necessarily will take place in the future using some shared mechanism of moderation. It is wise to embed the hooks to semantic descriptions in the design of new CVIS applications. This might take the form of a placeholder for a pointer to a (not yet existing) semantic description. This pointer preferably will have the form for an URI (universal resource identifier), a compact string of characters used to identify the source of a semantic description.

3. Cooperation architecture

3.1. Problem area

The cooperation architecture has to cope with various opportunities and threats that arise from trade offs that have to be made. Hereafter an enumeration of opportunities and threats is made that should be ticked off when taking decisions during trade offs.

Opportunities	Threats
<p>It allows multiple stakeholders to take part in this environment and lowers the barriers for new stakeholders entering.</p> <p>Private companies will have the opportunity to provide profitable services and system components and protect proprietary solutions to enable investments.</p> <p>Public stakeholders can fulfill their mission goals, specially if we think about large information dispatching.</p> <p>Public stakeholders will be able to provide same services to all users</p> <p>The public and private stakeholders will accomplish their goals to make the traffic more safe and efficient</p> <p>Services from complete different environments can plug into this world without rewriting</p> <p>The cost of the full deployment can be shared among different application domains and facilitate the overall return of investment</p>	<p>Increased risk of antagonistic system threats such as viruses, worms and Trojan horses</p> <p>Undesired services e.g. advertisements and spam</p> <p>Unsafe services</p> <p>Violation of privacy</p> <p>Data security issues such as user identification and authentication to prevent unauthorized usage</p> <p>Unreliable services</p> <p>Less robust services</p> <p>Lack of end-to-end responsibility of services causing quality-of-service problems and lack of ownership</p> <p>Open source software might get mixed into existing software, implying that proprietary software risks to be earmarked as being “open source” and hence causing loss of commercial willingness to invest</p> <p>Badly designed services causing performance problems of the overall system</p> <p>Lack of awareness during the design phase about issues related to concurrent execution of different applications (i.e. priority, sharing of resources, conflicts, etcetera)</p>

3.2. Solution directions

For the short term, that means the period during which the CVIS project runs, the solution for openness and interoperability lays in the construction of a fixed CVIS data model and appliance of a fixed set of well defined application interfaces and the framework offered by FOAM. For the long run, however, this approach will not provide a rigorous solution to an ever changing world.

The cooperation architecture for CVIS is based on various levels of interactions, comprising business models, business cases in the form of services offered, business protocols represented by contracts, service deployment and interconnection protocols. This is schematically depicted in Figure 1, together with the components delivered by CVIS or yet to be delivered in a later stage (world models).

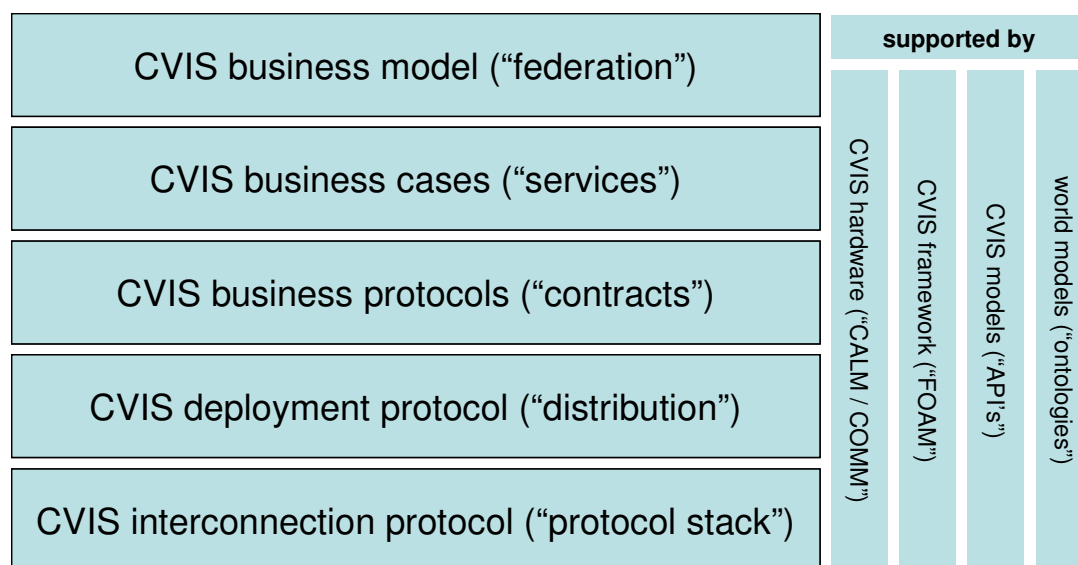


Figure 1, The CVIS cooperation stack and supportive components

3.3. Meta data registration

The set of well defined application interfaces and the framework offered by FOAM, together with the work done in the COMM subproject and based on CALM establish the base part of the cooperation stack. On top of this a mechanism must be set up to cope with the ever changing world. New business models will appear and old ones become obsolete. New concepts will evolve from old ones, the old ones becoming less frequently used and eventually obsolete. Naming will change, inconsistencies arise, etcetera. Coping with this imminent chaos necessitates maintenance on a more abstract level. This has been foreseen in the past, and already an initiative of the Highway Authorities in the UK has established an ITS Metadata Registry³ to foster harmonization across different systems and avoid re-invention and duplication of effort. The essence consists of a central registration and a

³ <http://www.itsregistry.org.uk>

voluntary adherence to a widely supported model of the ITS world. At the same time there is room for existence of a federation of ITS businesses with a certain degree of proprietary view upon the world, which is reflected in a granted compliancy level via a certification program.

The cooperation stack, in fact representing a series of contracts on top of each other, is within CVIS FOAM implemented as a tripartite interaction between the roles “service center”, “control center” and “service endpoints” (like a CVIS vehicle, a piece of roadside equipment or a nomadic device), see also Figure 2.

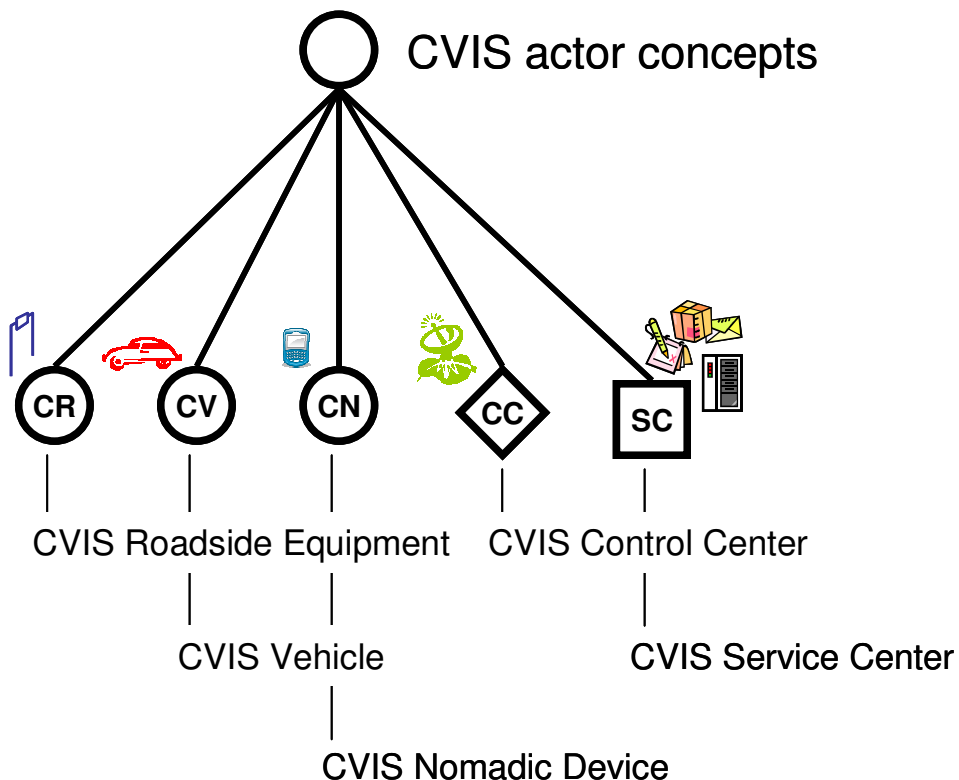


Figure 2, Various CVIS actor concepts and roles

The various roles and contracts are arranged into a service deployment role model. An example is depicted in Figure 3. From this example it can clearly be seen that the way businesses bind their customers is determining their market share (visualized by the colored dashed lines). He who knows how to bind the proper control centers gets the optimal market share. A company offering services for nomadic devices will have other interests than a business interested in services for specific roadside equipment.

Business will need to lean on (non-CVIS) services in order to streamline and secure their applications. This may vary from identity assurance in transactions to services like currently offered by the pilot project (see also section 2.2) implemented by Mott MacDonald on behalf of the Highways Agency (running until June 2008).

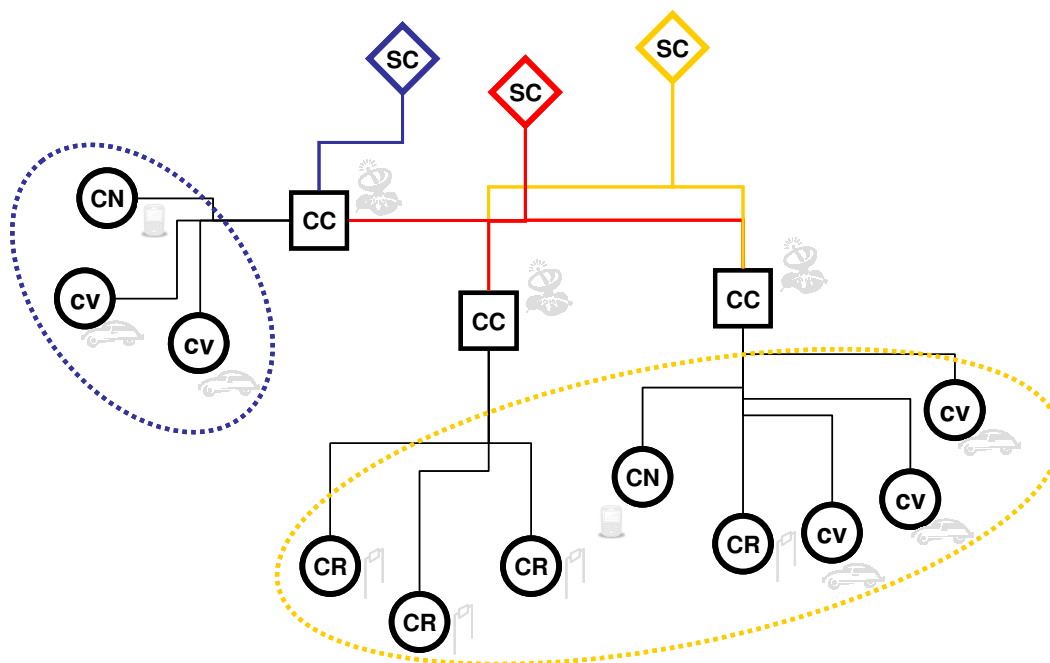


Figure 3, A CVIS service deployment role model example

Summarizing, the CVIS cooperation architecture will consist of the CVIS cooperation stack together with more generic, supplementary standards and services like (open) standards, a semantic model sharing service and secure interoperability by proper identity services (see also Figure 4).

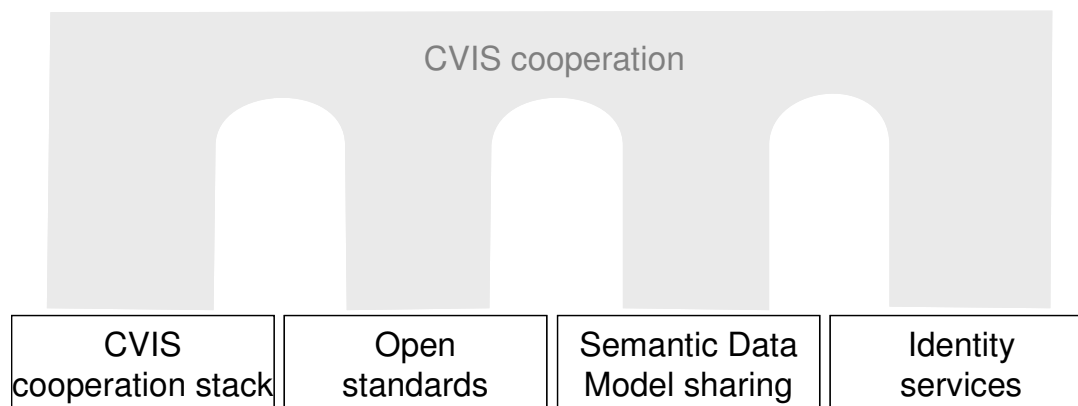


Figure 4, The CVIS cooperation architecture built on internal and external resources

4. Conclusions

- Something like “Good CVIS Development Practices” (i.e. guidelines or recommendations for development of sound CVIS applications that comply with the requirements imposed by the general CVIS framework) have yet to be made explicit
- Attention is required during application/service design with respect to the fact that other applications or services will run concurrently
- Attention is required with respect to possible threats during design trade offs when building on the CVIS cooperation architecture
- In order to guarantee the compliance with any standard CVIS specification, some sort of "CVIS Certification Process" should be developed
- Apart from the communication part within CALM / FOAM no provision yet exists within CVIS to deal with arbitration in sharing of limited resources by concurrent processes. It is highly recommended that such a mechanism will be devised.
- On the short term a fixed data model will suffice to establish interoperability and openness, but on the long term a more sophistic solution must be found. The CVIS cooperation stack and supportive components from CVIS provide a basis for such a long term solution.
- The use of semantics when establishing a rigorous solution for interoperability is without any doubt. In order to guarantee the interoperability with any established ITS protocol or system, some sort of "Meta Data Model Certification Process" should be in place. The institution setting up and maintaining that process does not necessarily be part of CVIS.
- The CVIS cooperation architecture leans upon three pillars that do not make part of the CVIS domain: open standards, semantic data model sharing and identity services. The latter two pillars will most likely be formed by independent third party bodies. Some contours of such bodies can already be seen to develop for the ITS world in general.