iTLC verification and certification

Process and joint environment for testing and certification of iTLC components in the Netherlands and Flanders

Versioning

Version	Date	Author	Status
0.1	1-10-2020	S. Boerma (MapTM)	Concept
0.2	20-10-2020	B. van der Veen (MapTM)	Concept
0.3	03-11-2020	S. Boerma (MapTM)	Concept
0.4	04-11-2020	J. Vreeswijk (MapTM)	Concept
0.5	04-11-2020	S. Boerma (MapTM)	1st release
1.0	03-12-2020	S. Boerma (MapTM)	2nd release
1.1	23-02-2021	W. Vandenberghe (imec) C. Moerbeek (AWV)	Concept
1.2	24-03-2021	W. Vandenberghe (imec)	Concept
1.2.1	25-03-2021	W. Vandenberghe (imec)	Concept
1.2.2	29-03-2021	W. Vandenberghe (imec)	Draft cleaned up for external dissemination
1.2.3	14-06-2021	J. Zee (AWV)	Concept, input working group processed
1.2.4	16-06-2021	J. Zee (AWV)	Cleaned
1.2.5	13-07-2021	J. Zee (AWV)	Comments working group iTLC testbed processed
1.2.6	15-07-2021	J. Zee (AWV)	Definitive
1.2.7	01-09-2021	J. Zee (AWV)	Definitive, Additional review comments processed
1.3	20-04-2021	J. Zee (AWV)	Clarification of the role of Information Service
1.9	02-06-2023	W. Vandenberghe (I&W)	Completely revised version based on WG Testbed decision on March 23, 2023
1.9.1	08-06-2023	W. Vandenberghe (I&W)	Reviews of the Netherlands-Flanders public support team processed
1.9.2	16/6/2023	W. Vandenberghe (I&W)	Input WG Testing Processed
1.9.3	29/6/2023	W. Vandenberghe (I&W)	Final input WG Testing processed 29/6
2.0.0	13/09/2023	J. Zee (AWV) W. Vandenberghe (I&W)	CAB feedback processed (editorial update: only typos and footnotes for abbreviations, no substantive changes)

Note: the above versioning table represents the versioning history of the original Dutch version of this document. The English translation of that original document does not get its own version, it is always released as the translation of a specific version of the Dutch one. This specific translation has been written by Jasper De Keukelare (imec), Bart Lowyck (imec) and Wim Vandenberghe (AWV). In case of any conflict between the content of this translated version and the original Dutch one, the Dutch document is the leading document.

Contents

1. Introduction

All partners within the iTLC ecosystem have an interest in the high-quality, reliable and predictable functioning of the entire traffic light influencing component chain. The success of the ecosystem stands or falls with the quality of the service, to which all chain partners must contribute. The data chain can only function properly as a whole if every link in that chain functions properly (i.e. in accordance with national and international standards, agreements and connection requirements) and continues to function. This also applies to changes to products, standards and agreements. This results in a concrete need for a thorough verification approach that shows that products were built according to the current specifications. This to mitigate problems in the roll-out and operation of the iTLC ecosystem, now and in the future. **Positive results of verification are confirmed in a certificate.** Products without a valid certificate are not allowed to participate in the production ecosystem.

This document contains the elaboration of the certification process for all components in the iTLC chain, as well as a brief description of the joint test environment, the so-called iTLC testbed. This elaboration is a thorough revision of the previous version (v1.3), based on the evaluation by WG Testing.

The added value of the elaborated certification process is to ensure as much as possible that a realized product correctly implements the underlying technical specifications and works functionally in the chain. However, it cannot give a 100% guarantee that certified products comply with every technical detail of that technical specification, or that no certified products exist that use a different valid interpretation of that technical specification. Even after successful certification, it remains the responsibility of the suppliers to make all necessary changes to their certified products including already deployed items on the street in the event of field issues.

1.1. Definition of the chain

Because of the cross-border cooperation between the Netherlands (Talking Traffic) and Flanders (Mobilidata) in the iTLC ecosystem, and the use of different names for the links in the chain in each region, the following name is used in relation to the testbed.

Link in the chain	Talking Traffic	Mobilidata
TLC	TLC (C1)	TLC
ITSApp	ITSApp (C1)	ITSApp
RIS	RIS (C1)	RIS
TrafficLightExchange	UDAP (C1)	MobilidataInterchange + RoadInfrastructureExchange
Service Provider	Cloud Service Provider (C2)	MobilityApplication ITS Backend
Information Service	App Provider (C3)	MobilityApplication ITS Frontend
Priority Service	PriorityBrokerConfigurator	TrafficLightPriority Configuration + TrafficLightPriority Validator
Road user sensing service	No specific term named	No specific term named
Road user sensors	No specific term named	No specific term named
Movable barriers	Physically movable barrier	No specific term named

Together, all these links form the iTLC chain as shown in the high-level architecture diagram below. In the same Figure 1 the interfaces between the different links are also indicated. Here too, there are differences between the Mobilidata and the Talking Traffic ecosystem domains:

Interface	Talking Traffic	Mobilidata	...
t1	TLC-FI	TLC-FI	
c1	Control Interface-TLC	Control Interface-TLC or ICU2-GPRS	
c2	Control Interface-APP	Control Interface-APP	
c3	Control Interface-RIS	Control Interface-RIS	
r1	RIS-FI	RIS-FI	
e1	SI[1]	SI	
e2	SI	MI,[2] II[3]	
e3	N/A	MI	
p1	Priority services	TrafficLightPriority	
s1	Proprietary interface and/or ITS-FMS	Proprietary interface	

[1] SI is the abbreviation of Subject Interface, the new name of UDAP-FI, which was adopted as part of Change Order 44 by the Strategic Committee at their 40th meeting as a new designation without substantive change.
[2] MI is the abbreviation of Mobilidata Interface, a superset of the C-Roads Basic Interface (BI).
[3] II is the abbreviation of Improved Interface, which was taken from C-Roads.

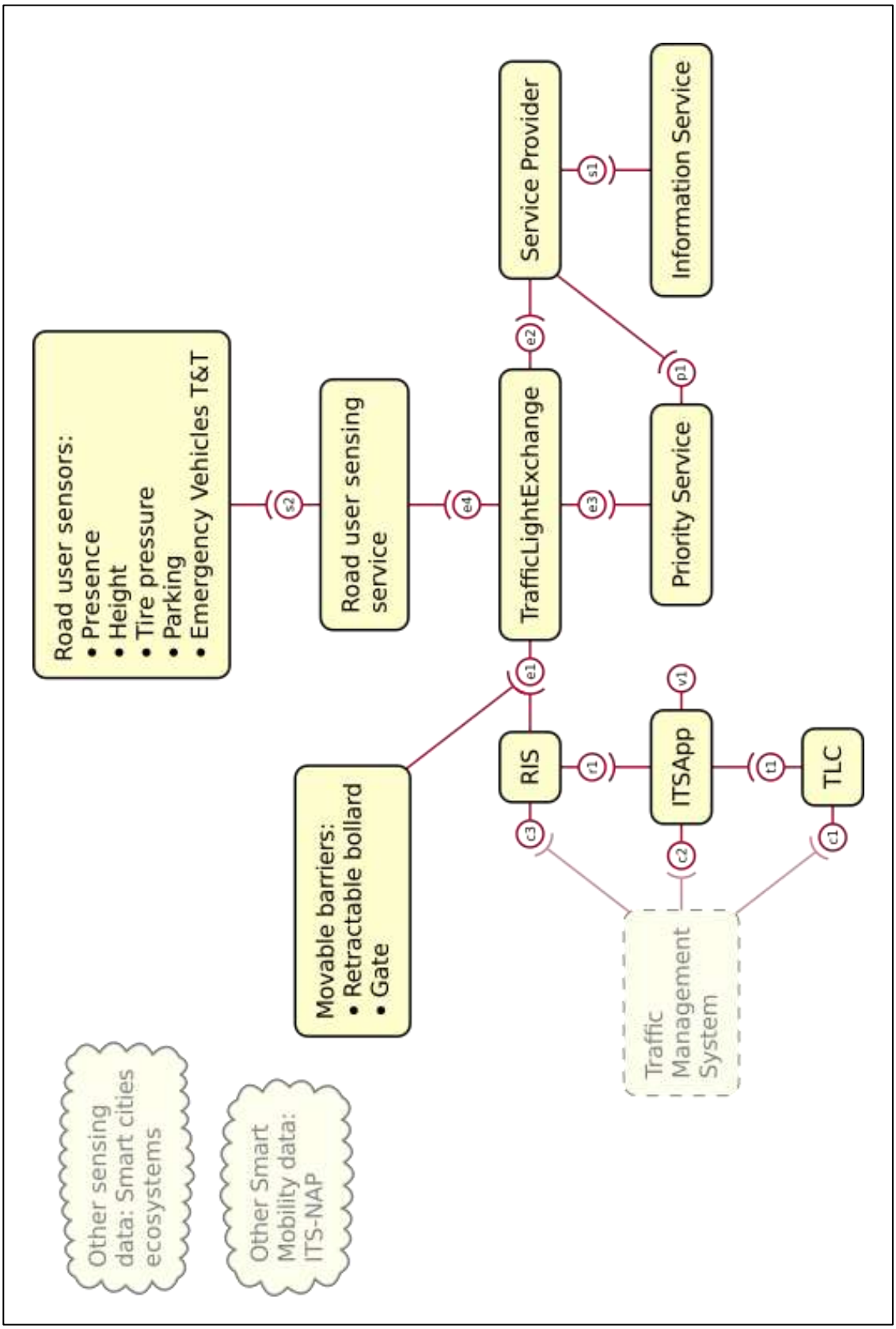

Figure 1: High-level architecture iTLC chain

Many of these interface specifications are published on the CROW knowledge platform[4]. However, the s1 interface between Service Provider and Information Service components is proprietary. As a result, there is no clear functional separation between the two types of components. This may vary depending on whether the Service Provider or the type of service varies. In the context of certification, the following (non-exhaustive) **functional separation between a Service Provider and an Information Service is used**:

- Information Service
  - Receives and displays up-to-date iTLC information
  - Sends timely location updates (GPS)
- Service Provider
  - Creates correct C-ITS messages (CAM/SRM/SRM0/...)
  - Processes C-ITS messages (SPaT/MAP/...)

This functional separation makes it clear that the **distinction between Information Service and Service Provider cannot be reduced to a distinction between cloud services and smartphone applications. Depending on the technical design, this boundary between the two can be very different.** For example, a client app on a smartphone can create correct C-ITS messages and process them all on the phone. That app should then be seen as both a part of the Service Provider (the component that creates and processes C-ITS messages), and as the entire Information Service (the components that collect the GPS data and present iTLC information to the user).

But another client app on the smartphone can, for example, limit itself to forwarding GPS updates to a backend, and expect that back-end to translate this GPS data into correct C-ITS messages (CAM, SRM, etc.) at the right time and then send it further down the chain on behalf of the app. In that case, the smartphone app is the Information Service, and the backend is the Service Provider and must be recognizable as such in the testbed.

The components in the iTLC chain can **support three different use case groups, each with their specific subcategories**:

- Prioritize
  - Public transport (P-PT)
  - Heavy trucks (P-HT)
  - Emergency vehicles (P-EV)
  - Convoy of road users (P-CV)
- Inform
  - Time to green and speed advice (I-TG)
  - Time to red and speed advice (I-TR)
  - Priority vehicle warning and waiting time (I-PW)
- Optimize
  - iTLC Traffic signal optimization (O-IS)
  - iTLC Traffic signal corridor optimization (O-CO)
  - Group of pedestrians (O-GP)
  - Group of cyclists (O-GC)
  - Group of vehicles (O-GV)

[4] https://www.crow.nl/thema-s/smart-mobility/landelijke-ivri-standaarden Dutch website - use Google translate

Each (partial) use case is aimed at one or more of the following **target groups**[5]:

- Motorized traffic (MT)
- Cyclists (C)
- Pedestrians (P)
- Emergency Vehicles (EV)
- Public Transport (PT)
- Heavy Trucks (HT)

As depicted in Figure 1 The classic iTLC chain with a focus on traffic lights was expanded with new types of components and services that also have to do with intelligent traffic management, such as roadside sensors, services that bundle information from roadside sensors and use them to publish information on the TrafficLightExchange, and physically movable barriers that can be controlled by Information Services via the TrafficLightExchange. All provisions in this document also apply to these types of components if they wish to be connected to the data chain. This ensures that these components must and can also be certified.

1.2. Verification

The primary need for verification is to determine whether iTLC products are built correctly according to the applicable iTLC specifications. This is to avoid as many problems as possible during roll-out in the field, and to encourage the embracing of iTLC solutions by the market and road authorities.

Verification is required for:
- **new products** in the chain (both from suppliers who are already connected to the chain, and from new suppliers who want to join for the first time)
- **new releases** of products in the chain (functional development, bug-fixing, compliance with new (versions of the) iTLC specifications, etc.)

Verification is divided into the following common test levels:

- **Unit testing:** These tests verify that one component meets the predetermined functional and non-functional requirements separately from the chain. Unit testing may use simulated input (mockup/stubs).
- **Integration testing:** In these tests, the functional interoperability with certain other components in the chain is tested for one component in the chain, typically these are the components to which this one component links in the chain. Simulated input (mockup/stubs) may be used for integration testing.
- **System testing:** During system testing, an entire chain is brought together and tested in its entirety for correct functional operation. Simulated input (mockup/stubs) may be used for system testing.
- **Acceptance testing:** During the acceptance test, an entire chain is tested in a production environment (on the street) for functional operation. Simulated input may not be used in acceptance testing.

[5] This has a link with the role/subrole concepts that are used in some exchanged ETSI messages in the chain.

The test levels have a sequential dependency. First, the Unit tests must be completed successfully, then the Integration tests can be started. After the Integration tests have been successfully completed, the System tests can then be started. Finally, after a well-completed System test, the Acceptance test is done.

1.3. Certification

The verification results must be recorded transparently and formally, so that it is very clear to all stakeholders in the chain whether a product in the iTLC chain has gone through all the necessary verification steps (and has therefore been built correctly according to the specifications). The instrument used for this is that of **certificates**. The associated certification process therefore includes all previously described test levels (Unit, Integration, System and Acceptance).

The following prerequisites apply:

- A certificate is required for every product that wants to join the iTLC chain. This applies to **all links** in the iTLC chain.
- Certificates have a **limited lifespan**, even if products do not change. In this way, it can be ensured that products continue to meet the current requirements over a longer period of time. If necessary, it can be decided that a certificate can be extended with limited verification if specifications and products remain unchanged.
- Certificates are only valid for a **specific version** of the product.

These principles are further elaborated in section 3.2.

2. The iTLC testbed

2.1. Testbed concept

The **iTLC testbed consists of all links in the iTLC chain** who have obtained or wish to obtain a valid iTLC certificate. It **is focused on the Integration and System Testing**. The Unit Testing and the Acceptance Testing are out of scope of the testbed. The **Unit tests are carried out in a proprietary test environment** of the supplier, the supplier's **Acceptance testing is done on-street**. Performance tests (if performance levels are required by technical specifications) are also outside the scope of the testbed: **Performance tests are always carried out on a proprietary test environment.** Run. This is summarised in Figure 2.

Information services that use an already certified Service Provider have the option to do Integration Tests and System Tests not on the testbed, but on the street if they wish. But in that case, they are obliged to apply in advance for the necessary permissions from the relevant road authority, and to take the necessary organisational measures to guarantee road safety (being physically present on site, providing extra traffic controllers, etc.). Due to this overhead and complexity, it is therefore not mandatory for this type of Information Services to use the testbed for certification, but it is strongly recommended.

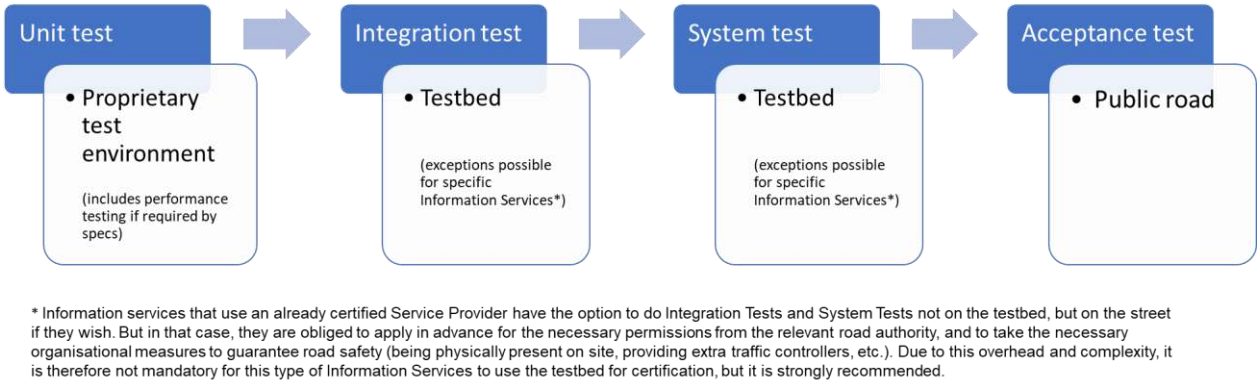

Figure 2: Relationship between test level and test environment

The joint testbed can be used by all chain partners without the direct involvement of other chain partners. At the same time, chain partners will not simply transfer their products completely to other (competing) parties for testing. An independent intermediate layer is needed that makes the components available in a uniform way without giving access to business-sensitive parts. For this reason, the testbed provides for the possibility for suppliers to make their products available from their own lab environment. In this way, a **distributed iTLC chain is created in the testbed**.

The iTLC testbed is a **permanent test environment that is available 24/7**. Support can be provided during business hours via the testbed manager[6]. This means that 24/7 support is not required from all chain partners. By means of a **testbed portal**[7] , it is clear to everyone which components are available for testing. Components in the testbed can be reserved for a certain period of time. In this way, parties can reserve a time slot for carrying out their tests.

In order to be able to fully set up this joint testbed and make it usable for all chain partners, **the following contribution to the test environment is required from the suppliers in the iTLC chain**:

- For all products from a supplier's portfolio with a valid iTLC certificate, **the supplier provides an instantiation for exclusive use in the distributed testbed** (from its own lab or hosting environment, or from the imec hosting environment where the testbed software also runs).
- The supplier **offers support when requested by the testbed manager**. To make the supplier's effort reasonable and equitable, the testbed manager operates as the first point of contact for all parties involved and is the only one who can escalate to the supplier. This minimizes the effort of the supplier.

The **testbed also offers added value as a test environment in addition to a certification environment**, both in terms of quality assurance in the chain and accessibility of the chain for new parties. However, certification tests have higher priority than other (development)

[6] The contact details of the testbed manager are kept up to date on https://dutchmobilityinnovations.com/spaces/1291/certificeren/wiki/view/51767/overzicht
[7] https://dev-ivri-portal.ilabt.imec.be/home

tests. When certification tests cannot be scheduled because all components are continuously reserved for other (development) tests, the testbed manager will, in consultation and based on a fair distribution, free up components for the purpose of the certification tests.

2.2. Support

The day-to-day management of this infrastructure is entrusted to the **testbed manager**. This provides **the first level support** to the users of the testbed (How do I reserve the testbed? Where can I find information about the resources? How do I bring in my own resources? Etc.). In addition, the testbed manager offers **second-level support** when tests do not run as expected and the tester himself cannot deduce where the error is located. If third-level support is required from another party in the chain, the testbed manager acts as a **single point of contact towards the other parties**. Furthermore, if components are not available when they should be, the testbed manager will contact the relevant party.

The **testbed manager is the gatekeeper for gaining access to the testbed**. New parties will only be granted access to the testbed by the testbed manager if they have demonstrated that their solutions under test are sufficiently mature. This can be done by an explanation of the unit tests that have already been carried out, live demonstrations in their own lab environment, etc.

As further described in section 3.1 the testbed manager **also takes an important role in the certification process itself. And also in the governance of testbed and process** the testbed manager has an important role to play (see section 2.3).

2.3. Governance

The governance of both the certification process and the testbed is taken up by the **Testbed User Group**. The group is open to representatives of both public and private parties with interests in the iTLC chain and among others works together on improved STD documents as a non-binding but useful tool for market parties. But also testbed-related matters such as testbed status (purpose, governance, implementation, etc.), further development, financing, etc. are formally taken up by this User Group. What comes out of this group **is formalized by the iTLC CAB and SC.** In order to keep this principle practically feasible, an appropriate distinction is made between strategic decisions (testbed status, certification process, etc.) that are actually formally submitted to CAB and SC, and operational decisions that fall within the mandate of the User Group for consideration without formal submission to the SC (adjustments to the STDs that have become non-binding, implementation choices of testbed, etc.). Also, the duration of existence of the User Group is under the authority of the SC. The principle is that it is tacitly renewed year by year, unless the SC calls a halt.

The **number of User Group meetings where decisions are made is limited to a maximum of once per quarter**. However**, the WG can meet more frequently (e.g. bi-weekly or monthly),** so that operational challenges can be responded to sufficiently quickly. But regarding strategic decisions that have to be made by CAB and SC, this can be arranged in such a way that the actual preparatory discussions are conducted in a bi- or multi-weekly rhythm, but the formal decision moments are very clearly planned in advance at a rhythm of

once a quarter. In this way, the participating parties can always delegate the right people to the User Group.

The operation of this User Group is supported by an **online collaboration platform, a community on the DMI platform called "Certification**".[8] As described on the wiki page of this community[9] , information about the activities within the Testbed User Group is made available, communication within the User Group is organized, and the current links to the testbed and contact details of the Testbed Manager are made available.

There is also a central place on this community **to share known problems and particularities of the testbed**, so that parties do not have to discover and solve the same problems again. To be clear: this is about problem management of the testbed itself. This does not concern individual issues that parties would experience with the testbed during testing, these are handled via the helpdesk functionalities of the testbed and are not transparent to other parties. The same applies to issues that are experienced with the components of other parties, first and second level support for these kinds of things is done via the testbed manager on a confidential basis. But this is about making certain identified problems with the testbed transparent (possibly as a result of one or more previously reported issues), and the further follow-up of these by those responsible for the testbed.

2.4. Funding

The certification process and supporting iTLC testbed has a public-private character. With this, the government aims to have as little impact as possible on the development activities of the private sector, but at the same time wants to provide a stamp of quality and therefore trust and to this end organise and guarantee a number of processes and agreements. This facilitation also includes further lowering the threshold for new players to enter the chain. After all, society does not benefit in the long term from a closed ecosystem in this area either.

The funding is therefore distributed as follows:

- **Market:**
    - Own component test environment (including functions to provide the necessary insights into the internal status of those components and to realize the necessary control, limited to what is needed to be able to test independently)
    - Manpower perform own tests, limited 3rd level support tests others
    - Voluntary participation in the Testbed User Group (improving the certification process, test specs, ...)
    - Supervision of the certification process (only for market parties that are members of the iTLC Strategic Committee)
- **Government**
    - Testbed software

[8] https://dutchmobilityinnovations.com/spaces/1291/certificeren
[9] https://dutchmobilityinnovations.com/spaces/1291/certificeren/wiki/view/51767/overzicht

        - Development financed by the Flemish Road Authority (AWV) and made available as open-source software, delivered in June 2021.
        - Technical software support
    - Hosting cost testbed
    - Testbed manager role (= day-to-day management of testbed, managing certification process, leading Testbed User Group)
    - Participation in the Testbed User Group (improving non-binding test specs, collecting feedback on testbed, ...)
    - Supervision of the certification process (as a member of iTLC SC)

No funding is provided by the joint governments for the 'out of pocket' costs of cloud parties, nor for the iTLC-specific tooling to be added to the testbed. These costs are seen as necessary investments by the market, which are part of the development and marketing of iTLC products and services. However, the possibility is offered to host free cloud services on the physical infrastructure of the (publicly-funded) testbed.

2.5. Requirements to bring in testbed resources.

The basic principle is that every certified actual version of a product must be made available for the testbed by the respective supplier. **No resource in testbed = validity of the certificate temporarily revoked until it is there**. This applies both to the initial contribution of the resource from the submission of the signed self-declaration (because that marks the point in time from which a resource must be made available in the testbed), and further during the validity term of the certificate. **Testbed manager checks for availability of the necessary resources.** However, this does take into account the possible exceptional situations formulated below.

If a supplier of a particular product has multiple certified versions of baseline specifications on the market, it is **only required to make the version of the product available in the testbed that implements the most recent baseline.** This means that over time, as the market evolves towards newer baselines, there are fewer and fewer opportunities to perform certification on old versions in the testbed. It is important that market parties are aware of this and include it in their own roadmaps. An example of how market parties can deal with this is to reach out to each other (possibly via the Testbed User Group) and make bilateral agreements about temporarily making previous versions available to each other again in the testbed. Another possibility is to carry out necessary tests related to previous versions that can no longer be found in the testbed on the road instead of on the testbed (with all the associated overhead such as obtaining permission from the road authority, providing sufficient human traffic controllers on site during testing to guarantee road safety, etc).

An exception to this rule is an Information Service that connects to the chain and uses an already certified service provider. The basic principle for this component remains that it must also be made available to third parties via the testbed, but only for this component (Information Service) and this situation (already using a certified service provider) **can be deviated from this once a motivated request has been approved by the testbed manager**. After assessing each motivated request, the testbed manager always

communicates the result (approved or rejected) to the SC. The criteria on which the testbed manager assesses this request include: availability of a different (but very similar) Information Service on the testbed that works with the same service provider (and therefore system testing with that service provider is possible), and whether or not the Information Service can be physically disconnected from a vehicle.

However, **even after such an exception has been granted, it must be possible to make this Information Service available on request as a resource to third parties for system testing.** In practice, this request is communicated by the testbed manager, who has first been informed by one or more market parties that the temporary availability in the testbed of this Information Service is necessary. The supplier then has the choice to make this Information Service temporarily available via the testbed, or if that is not possible or desired, he can choose to organize system tests on the street with this Information Service and the chain components that had expressed the need for this test. But in that case, the supplier of the Information Service not available on the testbed is obliged to take on all the overhead that a road test entails compared to a test on the testbed. This includes requesting the necessary permissions from the relevant road authority in advance, and taking the necessary organisational measures to guarantee road safety (being physically present on site, providing extra traffic controllers, etc.). Due to this overhead and complexity, it is therefore not mandatory for this type of Information Services to be able to make their resources available in the testbed, but it is strongly recommended.

Because of the proprietary interface between the Service Provider and the Information Service, **each Service Provider must include at least one Information Service or Test Tool with Information Service functionalities in the Testbed**. In this way, it is ensured that the complete iTLC chain is present in the testbed so that every supplier of a component can test the complete iTLC chain without the active involvement of other suppliers.

For each product in the iTLC chain defined in section 1.1 **preferably a dedicated instance of the certified product** shall be made available exclusively to the testbed. But **at a minimum, this can also be a logically separate domain on a production or acceptance environment**. In this case, the operation of the production or acceptance domain may not affect the operation in the testbed domain. This is the responsibility of the supplier. The supplier provides technical support at the request of the testbed manager.

Note: it is understandable that suppliers **want to combine domains for their own needs from the point of view of cost control. This is allowed as an exception to the requirement that any certified actual version of a product must be made available for the testbed by the relevant supplier, provided that a substantial amount of time remains available for the testbed.** In that case, an unambiguous registration must be made via the testbed about the (un)availability of the component.

To **make independent testing possible** (and thus to be able to limit the necessary support of the ecosystem for each supplier to third-level support), it is important that each user of the testbed can interpret whether a desired behavior was also observed during the test with the components other than their own product**.** In addition, the tester must also be able to set specific things on other components (e.g. setting detector high on a TLC). **For each resource, it is hence asked to provide a way to read out the status information that is relevant for the execution of integration or system tests by other parties, and to have specific things set up by the tester**. Which information needs to be made available for which type of component, and which things need to be able to be set up, is determined and documented together with the market in the WG Testbed and can be adjusted based on advancing insight. In doing so, necessity or desirability, feasibility and affordability are always

taken into account. Meeting these requirements is included in the assessment of whether a resource is present in the testbed.

The **way in which the components achieve this technically is a free choice, but the accompanying documentation must be made accessible via the testbed**. Examples of providing access for which the testbed offers support today are:

- unlocking a webpage built into the resource with status info and trigger options
- log in to the resource via Telnet or SSH via the testbed web page and execute the appropriate commands there
- visualization TLC status of the lights on the webpage of the testbed based on a Telnet IVERA link (other links can be added to the testbed by vendors)

3. The Certification Process

3.1. Process description

The entire certification process is depicted in Figure 3. It clarifies the roles and responsibilities of both the market parties, testbed manager and governments of specific ecosystem domains for which a certificate is requested. The summary of whom declares what during the process is:

- **Self-declaration by market party**
- **Assessment forms by testbed manager** (international testbed, international role)
- **Certificate by Public Authority(ies) of the ecosystem domain for which the certificate is issued.** The Public Authorities can individually decide how to give further substance to this. For example, testbed experts of AWV for the Flemish certificate and SC iTLC on behalf of I&W for the Dutch certificate.

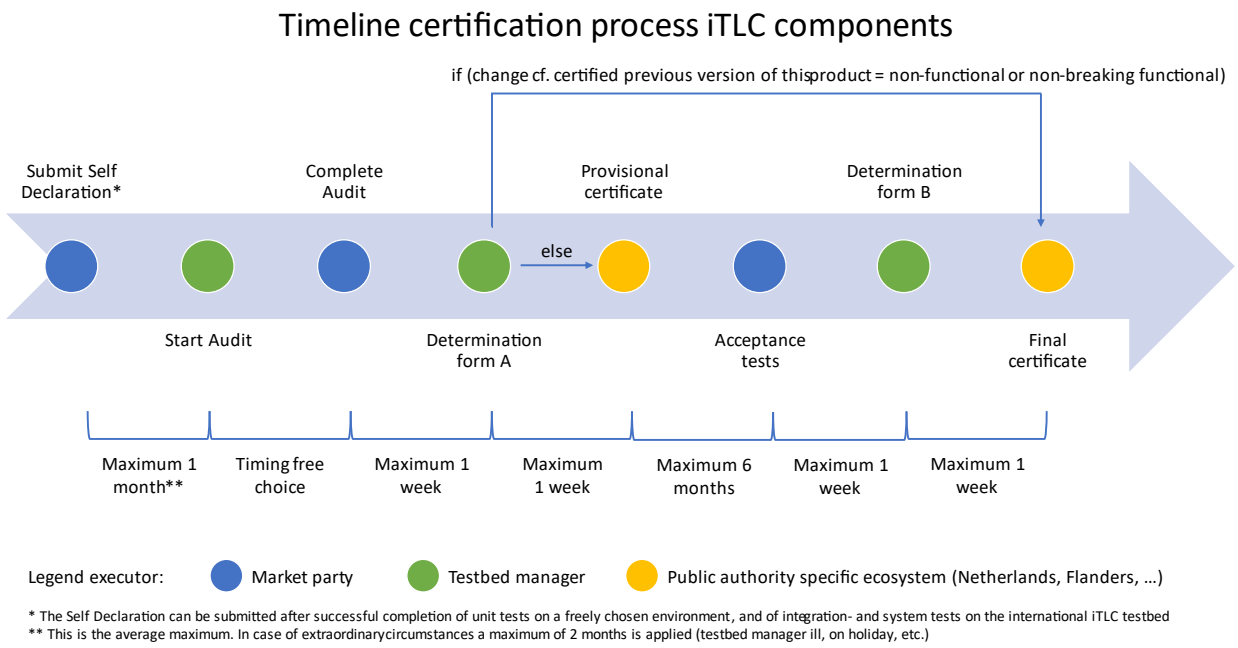

Figure 3: Formal certification process and timeline.

The basis of the certification process is the submission of a **self-declaration by the supplier of a product** in the iTLC chain, stating that they have carried out all the necessary verification steps associated with test levels Unit, Integration and System tests, and that based on the obtained results it can be concluded that the product has been implemented correctly according to the iTLC specifications.

Between the submission of the self-declaration and the provisioning of the certificate there is a period of on average maximum 1 month and in extraordinary circumstances two months in which the public authorities (= testbed manager) can start an Audit regarding specific parts of the self-declaration. Examples of such extraordinary circumstances are temporary unavailability of the testbed manager due to vacation, illness, family circumstances, etc. In that case of an audit, the parties may be asked to **demonstrate certain things on the testbed**. The existing Software Test Description documents (STDs) can be used as inspiration for this. New tests may also be needed, which will be added to STDs as living docs. This can be done at the request of both the testbed manager and the market parties involved. The living doc STDs are no longer published on CROW (and therefore no longer under the CAB/SC approval process), but are made available on the DMI community for certification.

To maximise the chance that in practice the lead time of this process is shorter than the maximum allowed term, market parties may in extraordinary cases proactively invite the testbed manager to attend their private testing preceding the submission of the self-declaration. Note: in the CAB there is an agreement that new technical specs are to be accompanied by corresponding test cases. These are to be integrated into the living doc STDs by the testbed manager. Added value is attributed to standardized unit test descriptions per component type. When elaborated by the current WG Tests (or possibly modified successor thereof), these will also be added to these living doc STDs. The testbed manager may also decide on the basis of a "hot topics" living document, to add test cases and/or to request extra audit actions.

The self-declaration can only be converted into a provisional certificate after full completion of the audit process, regardless of the associated lead time. In other words: the initiation of the audit has a lead time of 1 month (2 months in exceptional cases), but the execution of that audit does not have a fixed defined lead time. The provisional certificate will only be issued after successful completion of the unit, integration, and system tests.

To **move from a provisional to a definitive certificate, each party in the chain is asked to perform acceptance tests at minimum two different locations with two different iTLC configurations**[10]. And this for every target ecosystem domain. So for a certificate for Flanders: 2 iSATS in Flanders, for a certificate for the Netherlands: 2 iSATS in the Netherlands, for a certificate for both: 4 iSATS in total. These tests are carried out by all parties in a similar way, based on the national acceptance protocols iFAT/iSAT established by CAB/SC. These are currently designed for iTLCs, but will be adapted so that, in addition to the section "operation of the iTLC in the chain" (chapter 5 – iFAT/iSAT protocol), they can also be used to perform site acceptance tests of the other components in the chain. This elaboration will consider differences between the different target ecosystem domains and will stipulate who is responsible for which test.

This approach relies on the availability of an appropriate production environment of the chain to which the product to be certified can be connected for the execution of acceptance tests. This principle does not apply to the 2 unique central components of each ecosystem domain, being the TrafficLightExchange and PriorityService. Any update of these components cannot be limited to performing acceptance tests at a small selection of locations. After an update of these components, all other connected components in the chain are immediately affected. A different approach is required. Therefore **, for components of type TrafficLightExchange and PriorityService, it is not required to perform iSATS at specific locations as an acceptance test, but alternatively 3 months operation without incidents with source data of all components connected to the chain** is required before these products can be considered accepted.

One exception is allowed to this requirement to perform acceptance tests after the completion of the audit. In the event that the difference between the product or service to be certified and the certified previous version of that product or service is limited to the level of non-functional or non-breaking functional, then acceptance testing is not necessary, and after successful completion of the audit, a final certificate will be issued instead of a provisional certificate.

Note that the role of the testbed manager is central to the entire certification process. In case of unresolvable points of contention between suppliers and the testbed manager, the SC is the party to which escalations go.

This whole certification process was summarized in Figure 3, but also has an alternative mode of representation that is depicted in Figure 4. Both figures are equivalent in representation of the process and can be used at will.

[10] This means with different suppliers for one or more of the iVRI components TLC, RIS and ITS App

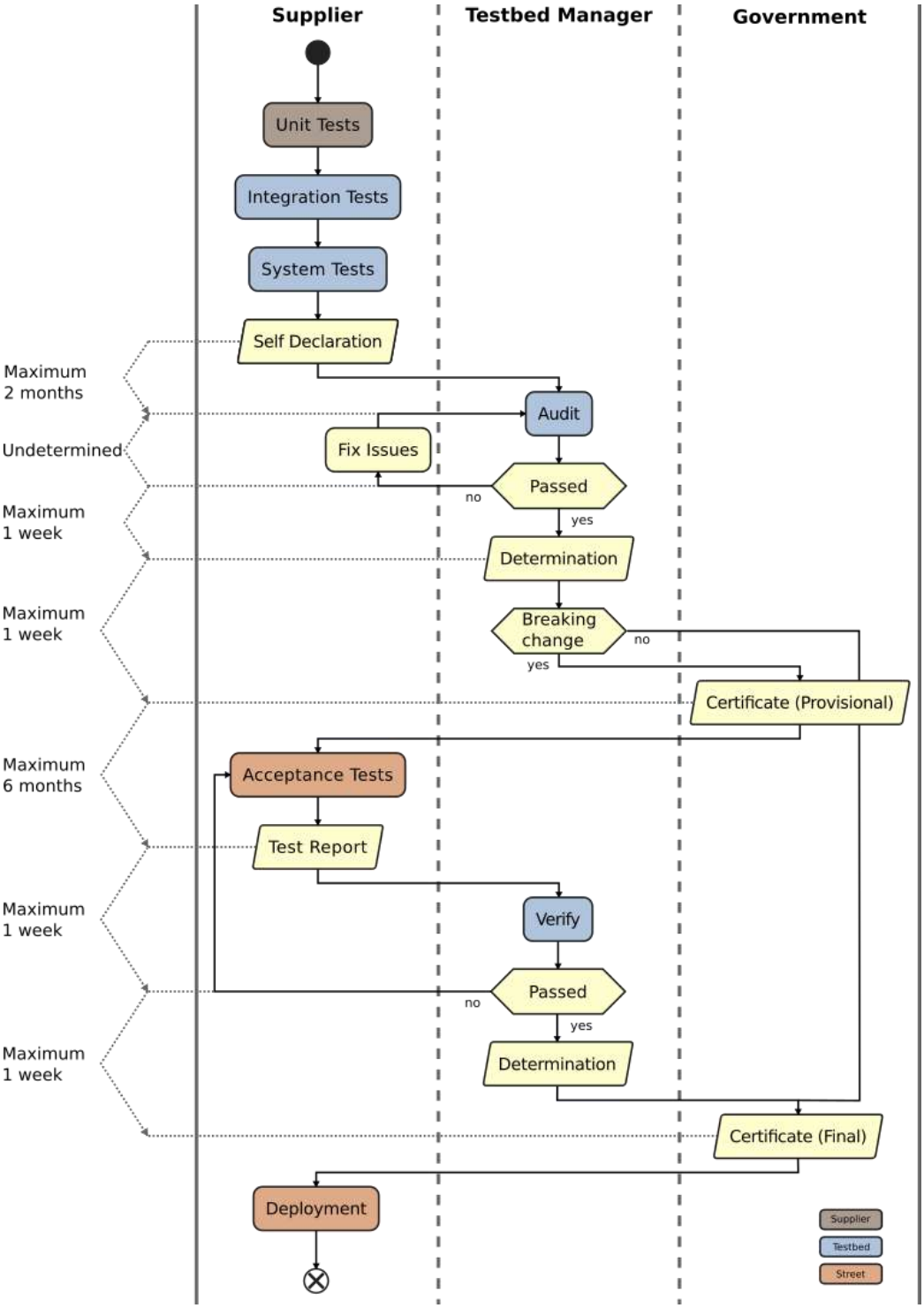

Figure 4: Alternative overview of the certification process and associated timeline. Colours are used to indicate the environment on which tests are executed in normal situations (see legend)

3.2. Certificate details

A certificate is issued per version of a component**, for a specific baseline of the specifications, for a specific use case(s) and target group(s)** [11] **and ecosystem** (Talking Traffic in the Netherlands, Mobilidata in Flanders, ...)**.** This way, there is the possibility to

[11] The definitions of the corresponding possibilities can be found in section 1.1.

proceed more quickly for part of the intended total functionality (subset use cases, subset target group), and it is made clear which technical regional differences the certified product does or does not meet. These differences are described in section 1.1

For the following types of components as defined in section 1.1 Certificates are provided:

- TLC
- ITSApp
- RIS
- TrafficLightExchange
- Service Provider
- Information Service
- Priority Service
- Roadside sensors
- Roadside Sensor Services
- Physically movable barriers

The **validity of a certificate is a maximum of one year** for a version of a product, from the date of issuance of the provisional certificate. This version relates to the components that contribute directly to the iTLC chain. **Parts that do not affect the operation in the iTLC chain fall are out of scope for certification**, and the changes to those parts therefore do not affect the version of the certified product. It is up to the supplier to keep these records. It is also the supplier's responsibility to upgrade the version of the certified product in the event of changes to the certified product as described below.

When a certificate is issued, a version number is assigned to the corresponding product. During the validity period of the certificate, the supplier in question can further develop this product. **Depending on the nature of changes to a certified product, recertification can be required** for this new version of the product. Three types of changes are defined:

- **Non-functional change**: for compatible bug fixes, security patches, etc. This has no impact on certification, no interaction with testbed manager required to be allowed to roll it out. In terms of certification, the version number of the product remains unchanged, but the internal version number of the supplier may change.
- **Non-breaking functional change** : in case of compatible changed functionality; only the changed functionality and proper functioning of the component at chain level must be verified (= tested) in the testbed before the valid certificate can be considered applicable to this new version of the product by the supplier. In terms of certification, the version number of the product remains unchanged, but the internal version number of the supplier may change. In that case, the supplier may also roll out this update immediately without first obtaining approval from the testbed manager. The documentation of this verification work, including release notes, must be submitted to the testbed manager after roll-out, in the form of a specific self-declaration. In case of doubts (both in case of field issues and insufficient verification of this change), the testbed manager has the right to initiate an audit, similar to that of the normal certification process.
- **Breaking functional change**: in the case of changes in which the modified product is no longer compatible with other components in the chain that have not yet been modified, or where the modified product has been modified so extensively internally that it can no longer be considered an update of an existing product, but that it must be seen as a new product. Recertification will have to be done before roll-out can

begin. In terms of certification, the version number of the product will then have to be changed, as well as the internal version number of the supplier.

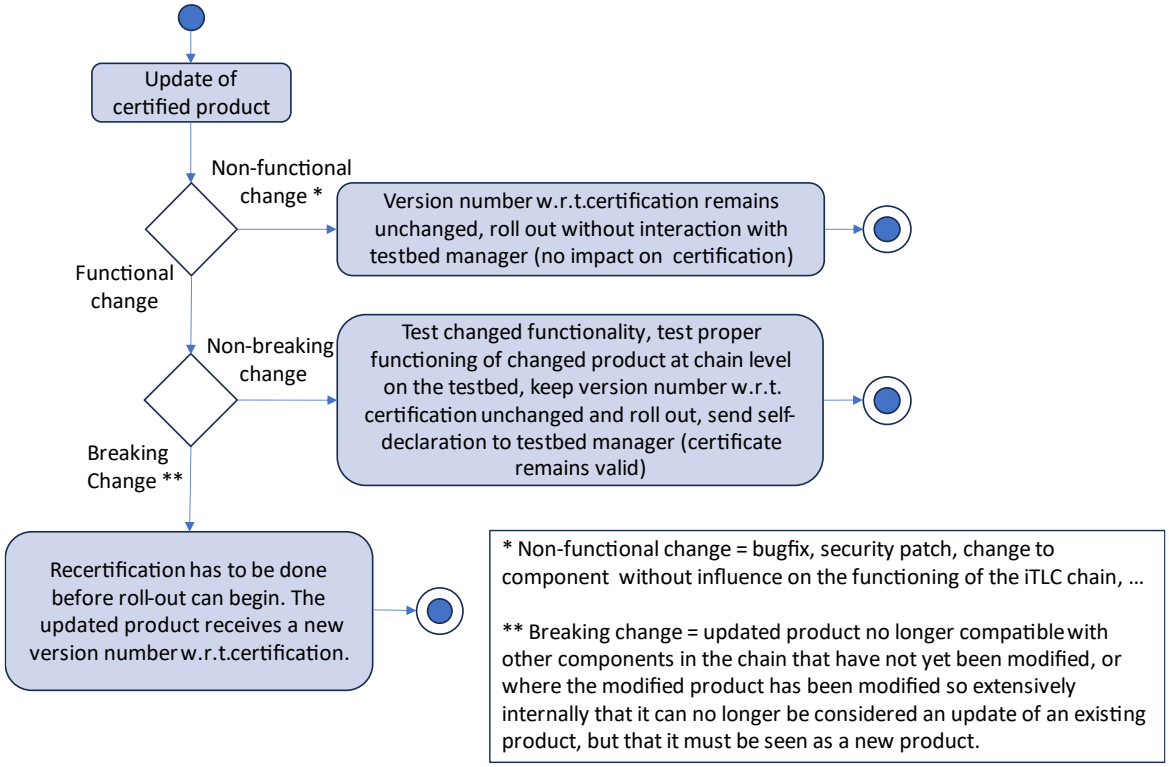

Figure 5: Relation between product updates and certificate validity

The **validity of the provisional certificate after successful completion of the unit, integration and system tests is 6 months**. During this period, the acceptance tests must be completed to convert the certificate into a final certificate. Parties that have obtained a provisional certificate but have not yet obtained a final certificate may therefore connect to the production environment during that period, but only for performing acceptance testing.

In case of changes (starting from non-functional change level) a complete re-certification must be done after the expiration of the validity of a certificate. **Only products that have not been changed (not even at non-functional level) can have their certificate extended without recertification**, provided that the chain specifications have remained unchanged. Note that in the process description it is stated that products with changes on patch- or Minor Level may skip the Acceptance Testing step, this for instance applies in the case of re-certification after one year.

For any certified product**, public authorities can temporarily pause the validity of a certificate in case of doubt because of field issues**, until it is demonstrated via a similar audit process that the product is okay. This applies to both provisional and final certificates. Given the impact this brings, public authorities will make sure that this measure will only be used with restraint. In the event of reported issues, an attempt to remove the doubts through direct interaction with the supplier will be undertaken first. This to avoid unnecessary usage of this measure.

3.3. Test case definitions

A previous version of this process description for iTLC certification included the obligation to carry out specific jointly defined test cases. These were described in specific documents (Software Test Descriptions, STDs). At that time, performing STDs was a requirement for successful self-declaration and subsequent certification.

However, this requirement is dropped. A self-declaration is no longer based on such jointly recorded STD documents. **Each supplier is free to choose which test cases are needed** to verify that the product in question has been built correctly to the specifications. But: t**he self-declaration must be based on actual own conducted testing**. The principle remains that these should include both unit testing (which are supplier and product specific, and hence free to choose and can be considered similar to self-acceptance testing), integration testing and system testing.

The existing (and potentially future improved versions of) STDs are delivered by the WG as a recommendation for own test work. The market parties involved in the WG are invited to jointly add an extra quality improvement and/or enrichment. In order to make it sufficiently clear how this has actually been implemented, it is required to add **a substantiation in free form** to this self-declaration that sufficiently illustrates the method used.

In summary : it is no longer necessary to carry out the joint STDs, but it is recommended. Substantiated self-assessment and the corresponding trust in suppliers is the basis of certification, in combination with mechanisms to allow swift government intervention should this trust be harmed.