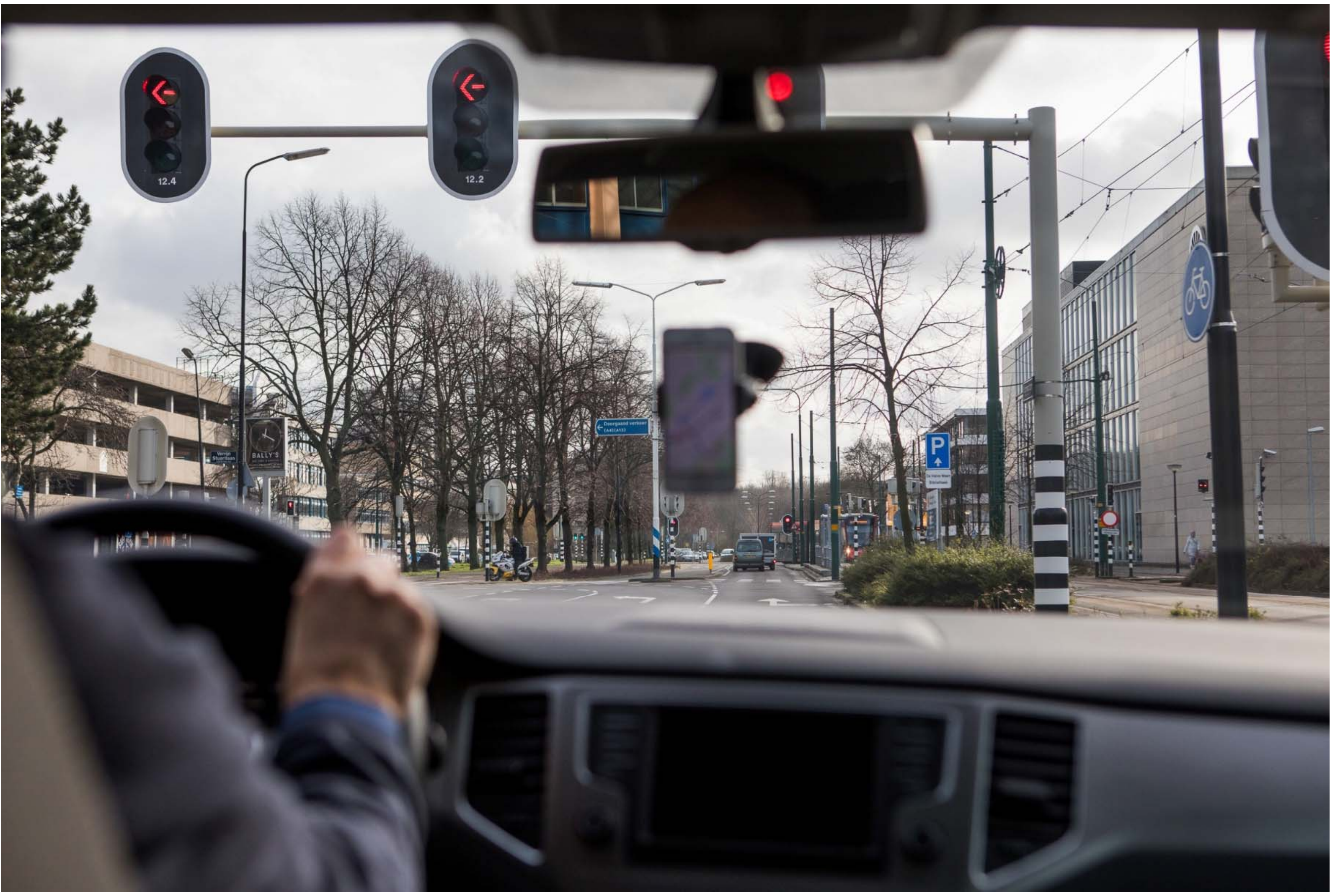
kennisplatform CROW

iVRI Security

Version 1.1



Over deze publicatie

De internationale ontwikkeling van Smart Mobility zorgt voor flinke vernieuwingen in verkeer, vervoer en mobiliteit. Dit raakt direct ook de verkeersregelinstallaties in de Nederlandse steden en provincies en op rijkswegen. Als verkeersregelinstallaties kunnen communiceren met voertuigen en weggebruikers kunnen weggebruikers worden geïnformeerd over actuele fasewisselingen van verkeersregelinstallaties en hierop hun rijgedrag vroegtijdig aanpassen, kunnen doelgroepen als openbaar vervoer, nood- en hulpdiensten en vrachtwagens conform beleidswensen van overheden worden geprioriteerd en kan data van voertuigen zelf worden gebruikt voor betere netwerkregelingen. Dit bevordert doorstroming, bereikbaarheid, verkeersveiligheid en duurzaamheid, legt de basis voor connected en automated driving en speelt in op een digitale samenleving waarin data en connectiviteit bijdragen aan economisch aantrekkelijke en duurzame steden.

Voor het effectief, veilig en leveranciers- en overheidsonafhankelijk communiceren van intelligente verkeersregelinstallaties (iVRI’s) met voertuigen en weggebruikers hebben bedrijven en overheden in het Innovatiepartnership Talking Traffic binnen internationale standaarden gezamenlijk specificaties en koppelvlakken voor iVRI’s vastgelegd. Eenduidig gebruik door alle overheden en betrokken bedrijven van deze uniforme afspraken binnen internationale standaarden is noodzakelijk voor interoperabiliteit en een goede en betrouwbare werking. Deze standaarden zijn daarom vastgesteld door de landelijke publiek private Strategic Committee ‘Borgen en beheren iVRI standaarden en producten’. Na vaststelling gelden deze standaarden voor alle bedrijven en overheden die in Nederland (willen gaan) werken aan iVRI’s t.b.v. intelligente mobiliteit. Vanuit de rol van onafhankelijk en landelijk kennisinstituut verzamelt CROW deze landelijk vastgestelde standaarden en stelt deze transparant ter beschikking aan overheden, adviesbureaus en leveranciers.

About this publication

The international developments in Smart Mobility technology are boosting innovations for traffic, transportation and mobility. This has a direct effect on traffic control systems in Dutch cities and provinces, as well as national highways. When traffic controllers are able to communicate with vehicles and road users, the latter can be informed about real-time phase changes in traffic lights, enabling them to anticipate and adjust driving behaviour accordingly. Also, special interest groups, such as emergency services, public transport and freight carriers, can be prioritized in line with public policy guidelines. The data provided by vehicles themselves can be utilised to improve network-based traffic control programmes. This has a positive effect on flow, accessibility, traffic safety and sustainability, laying out the fundamentals for connected and automated driving and preparing for a digital society in which data and connectivity contribute to economically viable and sustainable cities.

In order to let intelligent traffic controllers (iVRI) communicate with vehicles and road users in an effective, safe and platform independent way, businesses and governments have created and recorded common specifications and interfaces for iVRI technology. These are compliant to international standards and developed within the framework of the Talking Traffic Innovation partnership. The unambiguous use of these uniform agreements, within international standards, by all governmental bodies and businesses is necessary for interoperability and a good and reliable operation. These standards are adopted by the national public-private Strategic Committee ‘Ensuring and maintaining iVRI standards and products’. After adoption, these standards apply to all businesses and governmental bodies in the Netherlands that work, or plan to work, on iVRI technology for intelligent mobility purposes. Being an independent national knowledge institute, CROW collects these national standards and provides them to governments, consultants and suppliers in a transparent way.

Praktische kennis
direct toepasbaar

iVRI Security

Voorwoord

In mei 2016 is opdracht verstrekt door het Ministerie van Infrastructuur en Milieu via het Beter Benutten Vervolg (BBV) programma aan vijf VRA leveranciers om de in fase 1 opgeleverde iVRI architectuur, te bouwen en te testen in samenwerking met applicatiebouwers.

Dit document vormt Deliverable 1d van de afgesproken leverdelen in de opdrachtverstrekking en beschrijft de security requirements voor de ITS applicatie, de TLC en de RIS.

Dit document is tot stand gekomen door samenwerking van de vijf leveranciers in de werkgroep bestaande uit:

Koos van Vliet	dynniq energising mobility
Edwin Henning	KO HARTOG VERKEERSTECHNIEK B.V.
Eddy Verhoeven Hans Looijen	SIEMENS
Jaap Zee	swarco
Wim Nouwens Michel Huisman	Vialis®

NB. De rest van dit document is geschreven in het Engels om internationale uitwisseling te ondersteunen.

The rest of this deliverable has been written in English to facilitate international exchange.

Document control sheet

Document versions:

Version	Date	Author	Comment
0.9	2-7-2016	WG security	Final draft
1.0	25-8-2016	WG security	Final
1.1	13-10-2016	WG security	Final

Approval:

	Who	Date	Version
Prepared			
Reviewed			
Approved			

Publication level: Public

Version filename: iVRI2_deliverable_1d IRS security v1.1.docx

Contents

1 Introduction

This document describes the security requirements of the iTLC. In this chapter, a brief system overview will be given. See [Ref 3] for a detailed architecture description.

1.1 System overview

The iTLC architecture defines several interfaces of the iTLC. Figure 1 shows these interfaces.

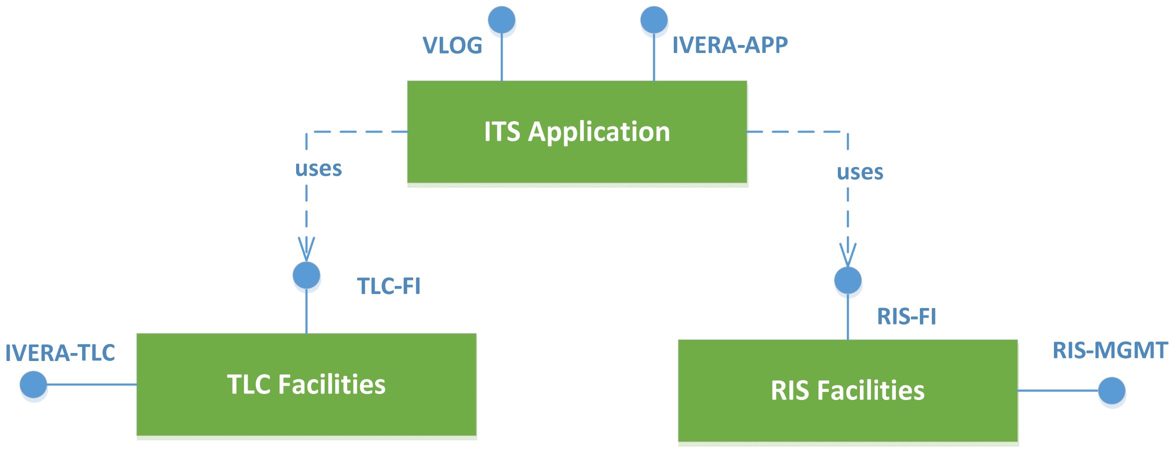


Figure 1 System overview

1.2 Document overview

1.2.1 Purpose

This document provides specifications of the security requirements of the iTLC architecture.

1.2.2 Document structure

Chapter 2 contains references to normative and informative documents.
Chapter 3 explains acronyms and used definitions and concepts.
Chapter **Fout! Verwijzingsbron niet gevonden.** outlines the security context.
Chapter 5 contains formal security requirements.

1.3 Advise for the reader

It is advised that the reader has taken knowledge of the iTLC Architecture as described in [Ref 3].

It is advised that the reader has a general understanding of cybersecurity also known as computer security[1].

[1] https://en.wikipedia.org/wiki/Computer_security

2 References

2.1 Normative

ID	Reference
[Ref 1]	*ETSI EN 302895, V1.1.1*
[Ref 2]	*CEN ISO/TS 18750:2015*
[Ref 3]	*Beter Benutten Vervolg, project iVRI, Deliverable F, iTLC Architecture, v1.2*
[Ref 4]	*SAE-J2735, Dedicated Short Range Communications (DSRC) Message Set Dictionary, SAE International - 2015-09*
[Ref 5]	*ISO/TS 19321:2015*
[Ref 6]	*ETSI EN 302 637-2 V1.3.2 (2014-11)*
[Ref 7]	*ETSI EN 302 637-3 V1.2.2 (2014-11)*
[Ref 8]	*RFC7525*[2]*, May 2015*

2.2 Informative

ID	Reference
[Ref 9]	*ETSI EN 302 665, V1.1.1*
[Ref 10]	*ETSI TS 102 894-2, V1.2.1*
[Ref 11]	*Rapportage onderzoek juridische inbedding Spookfiles A58*[3]*, December 2014*
[Ref 12]	*WaterISAC*[4]*, 10 Basic Cybersecurity Measures, June 2015.*
[Ref 13]	*Beter Benutten Vervolg, project iVRI Deliverable H2: iVRI Security & Safety matrix, version 1.2*

[2] https://tools.ietf.org/html/rfc7525

[3] www.spookfiles.nl/files/documenten/onderzoek_juridische_inbedding_spookfiles_a58.pdf

[4] https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

3 Acronyms, abbreviations and concepts

Acronyms and abbreviations

CEN	European Committee for Standardization
C-ITS	Cooperative ITS functionality for exchange of data between in-vehicle and or road side devices making use of either cellular or short range wireless communication
ETSI	European Telecommunications Standards Institute
FAT	Factory Acceptance Test
IDD	Interface Design Description
IRS	Interface Requirements Specification
ISO	International Organization for Standardization
iTLC (Dutch iVRI)	Intelligent TLC performing traffic light controller and C-ITS functions and providing access to these functions for ITS applications
ITS	Intelligent Transport Systems
ITS Station	Functional entity specified by the ITS station reference architecture (see *ETSI EN 302 665, V1.1.1*)
IVERA	Management protocol for traffic light controllers in the Netherlands
IVERA-APP	Management protocol for ITS applications.
IVERA-TLC	Management protocol supported by the RLC Facilities.
LAN	Local Area Network
PKI	Public Key Infrastructure
PoE	Power over Ethernet
RIS	See R-ITS-S
RIS-FI	R-ITS-S Facilities Interface
R-ITS-S	Roadside ITS Station, responsible for C-ITS functionality within a geographical area.
SAT	Site Acceptance Test
TLC	Traffic Light Controller; controls the signal of one or more intersections
TLC-FI	Traffic Light Controller Facilities Interface
TLS	Transport Layer Security
VLOG	Traffic Data log
VPN	Virtual Private Network
WAN	Wide Area Network

Concepts

ITS Control Application	A Traffic Control Application which uses TLC- and/or RIS-interfaces
ITS Application	An application which supports one or more ITS use-cases. Range of possible ITS Applications include an ITS Control Application
RIS Facilities	Component providing RIS Facilities to users (internal and/or external). Includes amongst others: - Access to information stored in the LDM - Services to trigger C-ITS messages
TLC Facilities	Component providing facilities of a TLC to users (internal and/or external). Includes amongst others: - Access to information from the TLC - Services to trigger actuators

4 Security context

The aim of iTLC is an open eco-system, standardized interfaces and clearly defined behaviour, allowing ITS applications to reside inside a roadside cabinet or in the 'cloud'. To facilitate this open eco-system security has to be integral to the design ('security by design').

This chapter outlines the security context of the iTLC and outlines the assumptions for the network in which the iTLC components are located.

4.1 Cyber security Best practices

Listed below are best practices regarding cyber security to reduce exploitable weaknesses and attacks on control networks. Please refer to the original article [Ref 12] for more information.

1. Maintain an accurate inventory of control system devices and eliminate any exposure of this equipment to external networks;
2. Implement network segmentation and apply Firewalls;
3. Use secure remote access methods;
4. Establish role-based access controls and implement system logging;
5. Use only strong passwords, change default passwords, and consider other access controls;
6. Maintain awareness of vulnerabilities and implement necessary patches and updates;
7. Develop and enforce policies on mobile devices;
8. Implement an employee Cybersecurity training program;
9. Involve executives in Cybersecurity;
10. Implement measures for detecting compromises and develop a Cybersecurity incident response plan.

4.2 Private network

The security requirements in this document are based on a system setup where the components of the iTLC architecture are located on a private network used for monitoring and controlling devices (IRS_SEC_GEN_001). The private network could spread across a city or an entire province and can be used to control and monitor a wide variety of objects (i.e. the network is not restricted to iTLC's only).

The assumption is made that the network is designed and maintained by a network administrator in accordance with the best practices outlined above, recognizing that a network administrator may have its own cybersecurity policy and best practices.

The network architecture and security measures for this (private) network are out of scope for this specification.

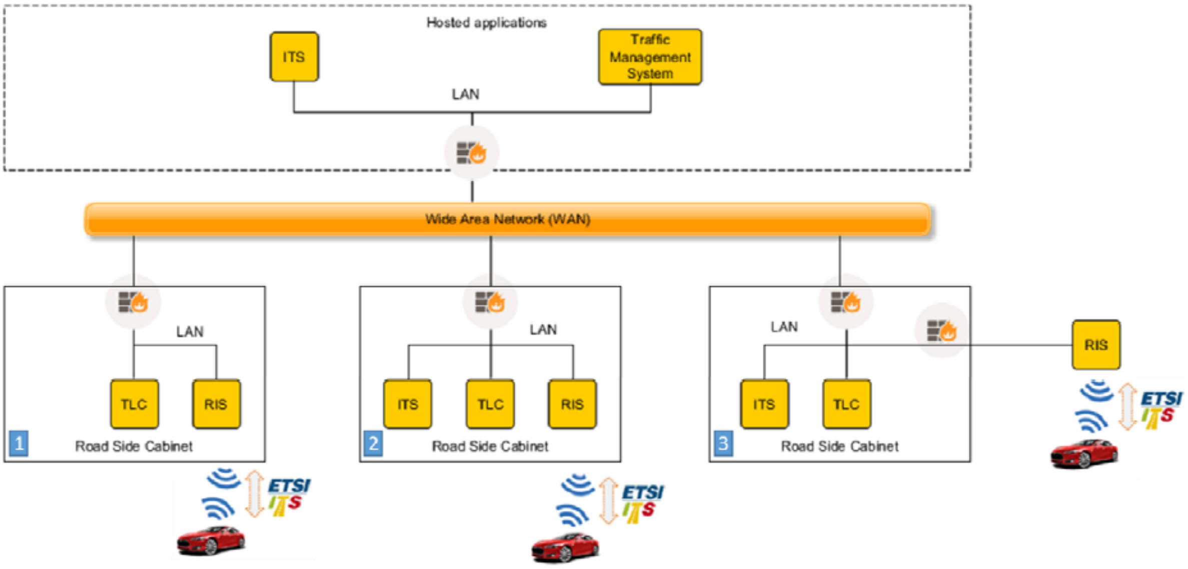


Figure 2 Private network overview

The figure shows several examples of connecting iTLC components to the private network:

1. The ITS application is hosted in the network and the TLC and RIS are located in the roadside cabinet [1].
2. All components are located inside the roadside cabinet [2]. Access to the iTLC components from the network can be restricted by an optional firewall integrated in the roadside cabinet.
3. The RIS or another device (connected to the LAN) is located outside the roadside cabinet [3]
4. A RIS using its own roadside cabinet [not shown].

4.3 Devices on the private network

The list below outlines the typical methods for connecting devices to the private network:

1. Connect a device to the LAN inside a roadside cabinet using an available network connector.
2. Connect a device to the LAN inside a server room using an available network connector.
3. Connect a device using a VPN (i.e. remote access by extending the private network across a public network or the internet).
4. Connect a device to a network connector outside the roadside cabinet. For example, a Power over Ethernet connector for interfacing with a pole mounted device.
5. Connect a device via a Wifi access point located inside a roadside cabinet or placed near a roadside cabinet.

Best practice: Maintain an accurate inventory of the devices on the private network.

4.4 Temporary devices on the private network

A device in this context can be a service laptop or another device used for diagnostic or maintenance. The list outlines typical methods for connecting temporary devices to the private network:

1. Connect a device to the LAN inside a roadside cabinet using an available network connector.
   a. After opening the main cabinet door.
   b. After opening the police panel door.
2. Connect a device to the LAN inside a server room using an available network connector.
3. Connect a device using a VPN (i.e. remote access by extending the private network across a public network or the internet).
4. Connect a device via a Wifi access point located inside a roadside cabinet or placed near a roadside cabinet.

Best practice: Develop and enforce policies on mobile devices.

4.5 Data exchange with devices outside the private network

Data is exchanged in a controlled manner with devices outside the private network. In a typical network there will be:

1. Centre-to-Centre data exchange (for example a link to the National Data Warehouse[5]) using a gateway.
2. Exchange of ETSI messages between the Roadside-ITS-Station and vehicles (i.e. ETSI messages via the RIS Wifi-p (IEEE802.11p) interface.).

Best practice: Eliminate any exposure of control devices to external networks.

4.6 Security matrix

In iVRI phase 1 a security and safety analysis has been conducted on this open eco-system and mitigating actions have been identified. The results are documented in [Ref 13].

[5] Nationale Databank Weg en verkeersgegevens

Listed below are identified security threats. The mitigation actions for these threats are addressed in the requirements in this document. The threats are sorted by risk (impact * probability). The list contains all threats with a risk >= 15 and a selection of the threats with a lower risk.

#	Threats	Impact	Probability
A1	Unauthorized persons that have direct or indirect (via applications) access to the iTLC.	5	5
A2	Authentication information becomes public due to irresponsible behavior of people.	5	5
A3	Cryptographic methods become outdated and are not being updated	4	5
A4	Incorrect permissions	5	3
A5	Unauthorized physical access to the system or network	5	3
A6	ITS G5 messages not signed	3	5
A7	Unworkable situation (impact on daily workflow) due to tight security measures, leads to bypasses of the security.	5	3
A8	Too many and complex security measures lead to incorrect implementation of the security measures.	5	3
A9	Security settings are not correctly configured/implemented, leading to lower security or even disabled security.	5	3
A10	ITS application cannot access TLC facilities or the RIS facilities.	5	3
A11	Theft of the security settings, to be used later for unauthorized access.	5	2
A12	Security measures are not tested during development.	3	3
A13	Brute force attack may disable a user account.	3	2

4.7 Authentication

The iVRI security is based on username/password (i.e. **what you know**). All - standardized and manufacturer specific - network interfaces of iTLC components shall be secured with a username/password as a minimum.

Each iTLC component has a management interface, allowing the users to be managed centrally by the network administrator.

Transport Layer Security (TLS) allows the ITS client to verify the identity of the TLC facilities or RIS facilities.

*Note: More enhanced authentication methods based on **something you have** (like a token) or even more sophisticated (**something you are**) are outside the scope of this document.*

Note: In a setup without TLS the system is sensitive to a man-in-the-middle-attack as the ITS application cannot authenticate the TLC Facilities and/or the RIS Facilities.

4.8 Cryptography

Transport Layer Security (TLS) is selected as a standard security measure on TLC-FI, RIS-FI, IVERA-TLC and IVERA-APP. TLS is strongly advised on all[6] other network interfaces of the components of the iVRI architecture.

(TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network. Major web sites use TLS to secure all communications between their servers and web browsers. The primary goal of the Transport Layer Security protocol is to provide privacy and data integrity between two communicating computer applications[7].

Note: In a setup without TLS the system is sensitive eavesdropping.

[6] VLOG3 is an output only stream without encryption.

[7] Source: https://en.wikipedia.org/wiki/Transport_Layer_Security

4.9 Certificates

As a consequences of choosing TLS, a public key infrastructure (PKI) is necessary for a client to authenticate a server (e.g. authentication of the TLC facility by an ITS application).

The public key infrastructure (PKI) is out of the scope for this specification.

Note[8]: A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

[8] Source: https://en.wikipedia.org/wiki/Public_key_infrastructure

5 Requirements

5.1 Introduction

This chapter contains security requirements of the iTLC-architecture as described in [Ref 3] and depicted in Figure 1.

5.1.1 Requirement notation format

The following format is used to define a requirement:

Req-ID	IRS-x-y-zzz
Title	
Description	
Source	
Comment	

- Req-ID: unique identification of the requirement according to the following format: 'IRS-x-y-zzz", where x is an identifier for the interface, y is a textual tag and zzz is a number of the requirement.
- Title: a short description of the requirement
- Description: formal and detailed description of the requirement.
- Source: reference to a source document used as input for the requirement.
- Comment: optional clarification of the requirement.

5.2 General requirements

The following requirements are applicable to security in general.

Req-ID	IRS_SEC_GEN_001
Title	Private network ('Secure bubble')
Description	The iTLC components, using the socket based TLC-FI and RIS-FI interfaces, shall be on a private network, managed by a network administrator, in accordance with cybersecurity best practices.
Source	Threat A1
Comment	The first line of defence is the access to the private network, both for systems and users.

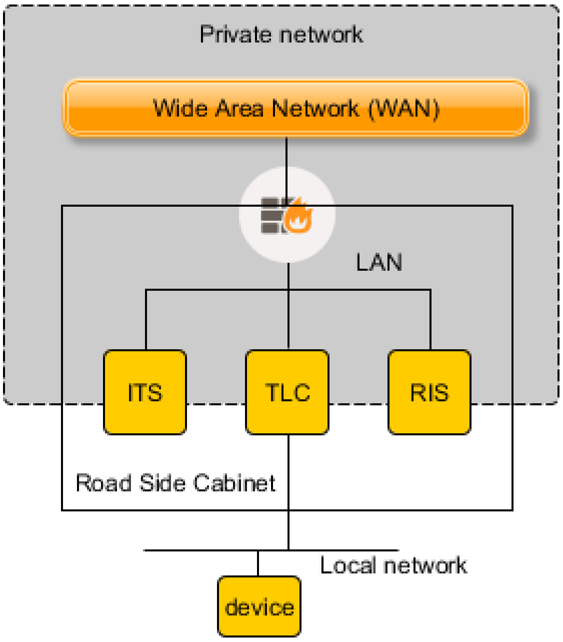
Req-ID	IRS_SEC_GEN_002
Title	Road side cabinet locks
Description	Roadside cabinets shall have locks and the keys shall be managed.
Source	Threat A5
Comment	People that have access to a roadside cabinet also have physical access to the network and can connect devices to the network.

Req-ID	IRS_SEC_GEN_003
Title	Alarm when roadside cabinet door is opened (optional for legacy controllers)
Description	When a roadside cabinet door is opened, an alarm shall be raised. The alarm shall be forwarded to the traffic management system (TMS) as an IVERA 'trigger event'. - Deur open politie panel (4012) - Deur open wegbeheerder (4013) - Deur open energie compartiment (4014)
Source	Threat A5
Comment	Legacy controllers may not have door contacts on all three doors. In the Traffic Management System the IVERA trigger event could be linked to a planned action by an authorized field engineer.

Req-ID	IRS_SEC_GEN_004
Title	Authentication
Description	A system or user shall authenticate itself using username and password when establishing any connection with an iTLC component (ITS application, TLC or RIS).
Source	Threat A1
Comment	Authentication: The act of verifying the identity of an entity (subject).

Req-ID	IRS_SEC_GEN_005
Title	Role based authorization
Description	A system or user shall be assigned a role, giving the system or user access to a predefined set of resources (objects) in the iTLC component.
Source	Threat A4, Best practice 4.
Comment	Authorization: The act of determining whether a requesting entity (subject) will be allowed access to a resource (object).

Req-ID	IRS_SEC_GEN_006
Title	Auditing
Description	A iTLC component (ITS application, TLC Facilities or RIS Facilities) shall keep a security audit log, including at least the following events: - Authorized access (start and end of the connection) - Failure to establish a connection. - Unauthorized access attempts. - Cabinet doors being opened and closed.
Source	Threat A1, A4
Comment	Logging access (including attempts to access) to the network interfaces of the components.

Req-ID	IRS_SEC_GEN_007
Title	Local (wired and wireless) networks.
Description	Local (wired and wireless) networks that reach outside the road side cabinet shall be protected to prevent illegal access to the private network. The supplier of the local network shall perform a security analysis and provide proof that the local network meets the security requirements set by the network administrator.
Source	Threat A1, A5
Comment	Take for example a pole mounted device with a Power over Ethernet (PoE) connection. Another example is a wifi network between devices on the street. These interfaces could be exploited to obtain access to the network. An example of a local network is depicted below. In the example the TLC uses a separate (local) network for connecting devices to the TLC.  Private network Wide Area Network (WAN) LAN ITS TLC RIS Road Side Cabinet Local network device

Req-ID	IRS_SEC_GEN_009
Title	User management
Description	An iTLC component (ITS application, TLC or RIS) shall have a management interface for user management. - Create a new user - Delete a user - Change a password User management shall be restricted to users with administrator rights.
Source	Threat A2
Comment	This setup allows the user management from a central location, giving the network administrator the possibility to implement a scheme for managing users. Examples of schemes are: - Assigning every authorized user a unique username/password. - Using role based username/passwords. - Changing passwords on a daily, weekly, monthly basis. - Etc. It is advised to separate user management from functional or technical management.

Req-ID	IRS_SEC_GEN_013
Title	Transport Layer Security (TLS)
Description	During the lifetime of equipment, the vendor should keep track of any systems not adhering to best practices as documented in RFC7525 [Ref 8].
Source	Threat A3
Comment	Over the last few years, several serious attacks on TLS have emerged, including attacks on its most commonly used cipher suites and their modes of operation. Because of these attacks, those who implement and deploy TLS need updated guidance on how TLS can be used securely.

Req-ID	IRS_SEC_GEN_014
Title	Product Development
Description	The security measures shall be tested prior to releasing a product or new product release for operational use. The supplier shall provide test results on request of the network administrator (i.e. the client).
Source	Threat A12
Comment	

Req-ID	IRS_SEC_GEN_015
Title	Site Acceptance Testing
Description	The security measures shall be verified during a SAT. This shall be a mandatory item on the SAT checklist.
Source	Threat A9
Comment	Default username/passwords are typically used for testing prior to the SAT. During the SAT the 'final' usernames/passwords are configured.

Req-ID	IRS_SEC_GEN_016
Title	Periodic security check
Description	The security measures shall be periodically verified in accordance with the security policy set for the private network.
Source	Threat A3, A9
Comment	This is the responsibility of the network administrator.

Req-ID	IRS_SEC_GEN_017
Title	Storing of security settings
Description	The security settings shall be securely stored in the iTLC components. More specific: - The security settings shall be stored in an encrypted format - The security settings shall not be accessible via an interface that does not meet the mandatory basic security requirements. - The security settings shall be accessible to administrators only.
Source	Threat A2, A11
Comment	

Req-ID	IRS_SEC_GEN_018
Title	Strong passwords
Description	The iTLC components (TLC Facilities, RIS Facilities and ITS applications) shall support strong passwords with a maximum length of 32 characters. A strong password is characterised by a minimal length, use of letters, digits and punctuation and is not sensitive to dictionary attack. Punctuation characters are restricted to the punctuation characters supported by IVERA-TLC and IVERA-APP.
Source	
Comment	A static strong password is considered safer than passwords that should be modified periodically.

5.3 Traffic Light Controller (TLC)

The following requirements are applicable to the security of the TLC.

Req-ID	IRS_SEC_TLC_001
Title	TLC-FI Authentication & Authorization
Description	An ITS client using TLC-FI shall be authenticated based on username and password. The ITS client shall be assigned a role (A Control, Provider or Consumer application). Access to the TLC resources shall be restricted based on the assigned role.
Source	Threat A1, A4
Comment	

Req-ID	IRS_SEC_TLC_003
Title	TLC-FI + TLS
Description	The TLC facilities shall support Transport Layer Security (TLS) on the TLC-FI interface, in accordance with the best practices document in RFC7525.
Source	Threat A1, A5
Comment	This is the mandatory security setup: 1. Restricted access to the private network 2. User authentication and authorization on the TLC-FI interface. 3. The ITS application can verify the identity of the TLC based on the provided (digital) certificate. 4. The communication between the ITS application and the TLC facilities is encrypted.

Req-ID	IRS_SEC_TLC_004
Title	IVERA-TLC Authentication & Authorization
Description	A client using IVERA-TLC shall be authenticated based on username and password. The client shall be assigned a role. Access to the TLC resources (objects) shall be restricted based on the assigned role.
Source	Threat A1, A4, IRS_SEC_GEN_004, IRS_SEC_GEN_005
Comment	The current IVERA pin code is deemed insufficient protection, especially since users and passwords are being managed using the IVERA-TLC interface. The login using a pin-code should be removed and replaced by a login using username and password, including objects to manage the users and passwords. The roles are defined in the IVERA specification.

Req-ID	IRS_SEC_TLC_005
Title	IVERA-TLC + TLS
Description	The TLC facilities shall support Transport Layer Security (TLS) on the IVERA-TLC interface in accordance with the best practices documented in RFC7525.
Source	
Comment	This is the standard security setup providing the following security: 1. Restricted access to the private network 2. User authentication and authorization on the IVERA-TLC interface. 3. The client can verify the identity of the TLC based on the provided (digital) certificate. 4. The communication between the client and the TLC is encrypted.

Req-ID	IRS_SEC_TLC_005a
Title	IVERA-TLC without TLS for legacy TLC
Description	A legacy TLC that cannot support TLS shall support IVERA-TLC without TLS.
Source	
Comment	

Req-ID	IRS_SEC_TLC_006
Title	Other TLC interfaces
Description	The manufacturer of the TLC shall provide a consolidated overview of the network interfaces of the TLC and the supported protocols, allowing the security risk of the equipment to be assessed. The network administrator may request a manufacturer to disable specific network interfaces due to the security risks associated to these network interfaces.
Source	Threat A1
Comment	The TLC can have other network interfaces like web pages, telnet, ftp, etc. Especially on legacy TLC's it may not be possible to bring all interfaces up to date with the latest security requirements. Basically the road authority together with the supplier of the legacy equipment has one of the following choices: - Allow a (less secure) network interface; - Disable a specific network interface (if at all possible); - Implement a secure alternative network interface (if at all possible); - Implement a TLS proxy; - Use a firewall to prevent access to a network interface from outside the roadside cabinet; - Ultimo replace the equipment.

Req-ID	IRS_SEC_TLC_007a
Title	User management TLC-FI
Description	The IVERA-TLC interface shall support the management of the TLC-FI users.
Source	IRS_SEC_GEN_009
Comment	

Req-ID	IRS_SEC_TLC_007b
Title	User management IVERA-TLC
Description	The IVERA-TLC interface shall support the management of the IVERA-TLC users.
Source	IRS_SEC_GEN_009
Comment	

Req-ID	IRS_SEC_TLC_007c
Title	User management File Transfer
Description	The IVERA-TLC interface shall support the management of users that are allowed to transfer files (upload/download files).
Source	IRS_SEC_GEN_009
Comment	*IVERA objects: FTPUSER.I, FTPPASS, FTPLOCATION.*

Req-ID	IRS_SEC_TLC_007d
Title	User management other interfaces
Description	The TLC shall have an interface to manage the users of other network interfaces (i.e. network interfaces for which the user management is not supported by IVERA-TLC).
Source	IRS_SEC_GEN_009
Comment	Think about interfaces like a secure shell or an integrated web server. The preferred option is to define manufacturer specific IVERA objects (like XSSHUSER.I, etc). Another option is a web interface for managing the users.

Req-ID	IRS_SEC_TLC_008
Title	Unique usernames
Description	Each entity of an ITS application shall have a unique username. The TLC facilities shall not accept a connection from an ITS application if there is already a connection with an ITS application with the same username.
Source	Threat A4
Comment	Prevent multiple ITS applications to setup concurrent TLC-FI connections using the same username. An event in the security audit can be linked to a specific entity.

Req-ID	IRS_SEC_TLC_009
Title	Security audit log
Description	The IVERA datacom events (6xxx) shall be used for the security audit logging.
Source	IRS_SEC_GEN_006
Comment	

5.4 Roadside ITS station (RIS)

The following requirements are applicable to the security of the RIS

Req-ID	IRS_SEC_RIS_001
Title	RIS-FI Authentication & Authorization
Description	An ITS client using RIS-FI shall be authenticated based on username and password. The ITS client shall be assigned a role. Access to the RIS resources shall be restricted based on the assigned role.
Source	Threat A1, A4
Comment	The roles are defined in the RIS-FI interface design description.

Req-ID	IRS_SEC_RIS_003
Title	RIS-FI + TLS
Description	The RIS facilities shall support Transport Layer Security (TLS) on the RIS-FI interface, in accordance with the best practices outlined in RFC7525 [Ref 8].
Source	Threat A1,A5
Comment	This is the mandatory security setup providing the following security: 1. Restricted access to the (virtual) private network 2. User authentication and authorization on the RIS-FI interface. 3. The ITS application can verify the identity of the RIS facilities based on the provided (digital) certificate. 4. The communication between the ITS application and the RIS facilities is encrypted.

Req-ID	IRS_SEC_RIS_004
Title	User management
Description	The RIS-MGMT interface shall support the management of users: - RIS-FI users - RIS-MGMT interface The RIS-MGMT interface shall be documented and available to third parties allowing the users to be managed centrally.
Source	
Comment	The RIS does not have a standardized management interface (like IVERA-TLC on the TLC).

Req-ID	IRS_SEC_RIS_005
Title	RIS-MGMT + TLS (optional)
Description	The RIS shall support Transport Layer Security (TLS) on the RIS-MGMT interface, in accordance with the best practices outlined in RFC7525 [Ref 8].
Source	Threat A1,A5
Comment	

Req-ID	IRS_SEC_RIS_006
Title	Unique usernames
Description	Each entity of an ITS application shall have a unique username. The RIS facilities shall not accept a connection from an ITS application if there is already a connection with an ITS application with the same username.
Source	Threat A4
Comment	Prevent multiple ITS applications to setup concurrent RIS-FI connections using the same username. An event in the security audit can be linked to a specific entity.

Req-ID	IRS_SEC_RIS_007
Title	IEEE802.11p / Wifi-p
Description	It shall not be possible to access the private network via the Wifi-p interface of the RIS. The Wifi-p interface shall be restricted to exchanging ETSI message using the GeoNetworking protocol stack (i.e. only allow 802.11p frames with Ethertype 0x8947, according to http://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml)
Source	Threat A1, A5
Comment	IPv6 and IPv4 shall be disabled on the Wifi-p interface of the RIS.

5.5 ITS application

The following requirements are applicable to the security of the ITS applications.

Req-ID	IRS_SEC_ITS_002
Title	TLC-FI + TLS
Description	An ITS application shall support TLC-FI + TLS.
Source	IRS_SEC_TLC_003
Comment	TLC-FI with mandatory security measures.

Req-ID	IRS_SEC_ITS_004
Title	RIS-FI + TLS
Description	An ITS application shall support RIS-FI + TLS.
Source	IRS_SEC_RIS_002
Comment	RIS-FI with mandatory security measures.

Req-ID	IRS_SEC_ITS_005
Title	TLC-FI and RIS-FI management
Description	An ITS application shall provide an interface, allowing an administrator to configure the TLC-FI and/or RIS-FI connections. - IP address/URL of the TLC's and RIS's. - Username and password for each connection.
Source	
Comment	Support initial configuration and changes during the life span of the system. The interface could be a standardized interface like IVERA-APP (IRS_SEC_ITS_009a) or a manufacturer specific interface.

Req-ID	IRS_SEC_ITS_006
Title	IVERA-APP Authentication & Authorization
Description	A client using IVERA-APP shall be authenticated based on username and password. The client shall be assigned a role. Access to the ITS application resources (objects) shall be restricted based on the assigned role.
Source	Threat A1, A4, IRS_SEC_GEN_004, IRS_SEC_GEN_005
Comment	The current IVERA pin code is deemed insufficient protection, especially since users and passwords are being managed using the IVERA-APP interface. The login using a pin-code should be removed and replaced by a login using username and password, including objects to manage the users and passwords. The roles are defined in the IVERA specification.

Req-ID	IRS_SEC_ITS_007
Title	IVERA-APP + TLS
Description	An ITS application shall support Transport Layer Security (TLS) on the IVERA-APP interface in accordance with the best practices documented in RFC7525.
Source	
Comment	This is the mandatory security setup providing the following security: 1. Restricted access to the private network 2. User authentication and authorization on the IVERA-APP interface. 3. The client can verify the identity of the ITS application based on the provided (digital) certificate. 4. The communication between the client and the ITS application is encrypted.

Req-ID	IRS_SEC_ITS_007a
Title	IVERA-APP without TLS in legacy TLC
Description	A legacy TLC that uses IVERA-APP to manage a backup application in the TLC shall use IVERA-APP without TLS, in case the TLC cannot support TLS.
Source	
Comment	

Req-ID	IRS_SEC_ITS_008
Title	Other ITS application interfaces
Description	The manufacturer of the ITS application shall provide a consolidated overview of the network interfaces of the ITS application and the supported protocols, allowing the security risk of the equipment to be assessed. The network administrator may request a manufacturer to disable specific network interfaces due to the security risks associated to these network interfaces.
Source	Threat A1
Comment	

Req-ID	IRS_SEC_ITS_009a
Title	User management TLC-FI and RIS-FI using IVERA-APP
Description	The IVERA-APP interface shall support the configuration the TLC-FI and/or RIS-FI connections. - IP address/URL of the TLC's and RIS's. - Username and password for each connection.
Source	IRS_SEC_ITS_005
Comment	

Req-ID	IRS_SEC_ITS_009b
Title	User management IVERA-APP
Description	The IVERA-APP interface shall support the management of the IVERA-APP users.
Source	IRS_SEC_GEN_009
Comment	

Req-ID	IRS_SEC_ITS_009c
Title	User management FTP
Description	The IVERA-APP interface shall support the management of users that are allowed to transfer files (upload/download).
Source	IRS_SEC_GEN_009
Comment	*IVERA objects: FTPUSER.I, FTPPASS, FTPLOCATION.*

Req-ID	IRS_SEC_ITS_009d
Title	User management other interfaces
Description	An ITS application shall have an interface to manage the users of other network interfaces (i.e. network interfaces for which the user management is not supported by IVERA-APP).
Source	IRS_SEC_GEN_009
Comment	Think about interfaces like a secure shell or an integrated web server. The preferred option is to define manufacturer specific IVERA objects (like XSSHUSER.I, etc). Another option is a web interface for managing the users.

Req-ID	IRS_SEC_ITS_010
Title	Security audit log
Description	The IVERA datacom events (6xxx) shall be used for the security audit logging.
Source	IRS_SEC_GEN_006
Comment	

Appendix 1. Requirements overview

As a reference, below all requirements are listed.

IRS_SEC_GEN_001	Private network ('Secure bubble')	13
IRS_SEC_GEN_002	Road side cabinet locks	13
IRS_SEC_GEN_003	Alarm when roadside cabinet door is opened (optional for legacy controllers)	13
IRS_SEC_GEN_004	Authentication	14
IRS_SEC_GEN_005	Role based authorization	14
IRS_SEC_GEN_006	Auditing	14
IRS_SEC_GEN_007	Local (wired and wireless) networks.	15
IRS_SEC_GEN_009	User management	16
IRS_SEC_GEN_013	Transport Layer Security (TLS)	16
IRS_SEC_GEN_014	Product Development	16
IRS_SEC_GEN_015	Site Acceptance Testing	16
IRS_SEC_GEN_016	Periodic security check	16
IRS_SEC_GEN_017	Storing of security settings	17
IRS_SEC_GEN_018	Strong passwords	17
IRS_SEC_TLC_001	TLC-FI Authentication & Authorization	17
IRS_SEC_TLC_003	TLC-FI + TLS	17
IRS_SEC_TLC_004	IVERA-TLC Authentication & Authorization	18
IRS_SEC_TLC_005	IVERA-TLC + TLS	18
IRS_SEC_TLC_005a	IVERA-TLC without TLS for legacy TLC	18
IRS_SEC_TLC_006	Other TLC interfaces	18
IRS_SEC_TLC_007a	User management TLC-FI	19
IRS_SEC_TLC_007b	User management IVERA-TLC	19
IRS_SEC_TLC_007c	User management File Transfer	19
IRS_SEC_TLC_007d	User management other interfaces	19
IRS_SEC_TLC_008	Unique usernames	19
IRS_SEC_TLC_009	Security audit log	19
IRS_SEC_RIS_001	RIS-FI Authentication & Authorization	20
IRS_SEC_RIS_003	RIS-FI + TLS	20
IRS_SEC_RIS_004	User management	20
IRS_SEC_RIS_005	RIS-MGMT + TLS (optional)	20
IRS_SEC_RIS_006	Unique usernames	21
IRS_SEC_RIS_007	IEEE802.11p / Wifi-p	21
IRS_SEC_ITS_002	TLC-FI + TLS	21
IRS_SEC_ITS_004	RIS-FI + TLS	21
IRS_SEC_ITS_005	TLC-FI and RIS-FI management	21
IRS_SEC_ITS_006	IVERA-APP Authentication & Authorization	22
IRS_SEC_ITS_007	IVERA-APP + TLS	22
IRS_SEC_ITS_007a	IVERA-APP without TLS in legacy TLC	22
IRS_SEC_ITS_008	Other ITS application interfaces	22
IRS_SEC_ITS_009a	User management TLC-FI and RIS-FI using IVERA-APP	22
IRS_SEC_ITS_009b	User management IVERA-APP	23
IRS_SEC_ITS_009c	User management FTP	23
IRS_SEC_ITS_009d	User management other interfaces	23
IRS_SEC_ITS_010	Security audit log	23

Colophon

iVRI Security

Published by
Talking Traffic

Date
13 Oktober 2016

Status
Final

Version number
1.1

CROW number
D3047-3

kennisplatform CROW