

Issuing Authority:	Owner:	Project Editor:
ITSO	Technology at ITSO	ITSO Head of Technology
Document number	Part Number:	Sub-Part Number
ITSO TS 1000	11	
Issue number (stage):	Month:	Year
2.1.4	December	2010
Title:		
ITSO TS1000-11 <i>Interoperable public transport ticketing using contactless smart customer media – Part 11: Remote POST</i>		
Replaces Documents:		
This is a new Part to the ITSO specification		

Revision history of current edition

Date	ITSO Ref.	Editor ID	Nature of Change to this Document (or Part)
September 2010	TS1000-11	MPJE	New document created

Document Reference: ITSO TS 1000-11

Date: 2010-12-20

Version: 2.1.4

Ownership: ITSO

Secretariat: Technology at ITSO

Project Editor: Mike Eastham

ITSO Technical Specification 1000-11 – Interoperable public transport ticketing using contactless smart customer media – Part 11: Remote POST

ISBN: 978-0-9548042-4-4

"Published for the Department for Transport under licence from the Controller of Her Majesty's Stationery Office. DfT does not guarantee the accuracy, completeness or usefulness of that information; and it cannot accept liability for any loss or damages of any kind resulting from reliance on the information or guidance this document contains.

© Queen's Printer and Controller of Her Majesty's Stationery Office, 2010, except where otherwise stated.

Copyright in the typographical arrangement rests with the Crown.

This publication, excluding logos, may be reproduced free of charge in any format or medium for non-commercial research, private study or for internal circulation within an organisation. This is subject to it being reproduced accurately and not used in a misleading context. The copyright source of the material must be acknowledged and the title of the publication specified.

For any other use of this material, apply for a Value Added Click-Use Licence at www.opsi.gov.uk/click-use/index.htm or e-mail licensing@opsi.gov.uk.

Foreword

This document is a part of ITSO TS 1000, a Specification published and maintained by ITSO, a membership company limited by guarantee without shareholders. The membership of ITSO comprises transport organisations, equipment and system suppliers, local and national government. For the current list of members see the ITSO web site www.itso.org.uk

ITSO TS 1000 is the result of extensive consultation between transport providers, sponsors, system suppliers and manufacturers. The Department for Transport (DfT) has also contributed funding and expertise to the process.

Its purpose is to provide a platform and tool-box for the implementation of interoperable contactless smart Customer Media (CM) public transport ticketing and related services in the UK in a manner which offers end to end loss-less data transmission and security. It has been kept as open as possible within the constraints of evolving national, European and International standards in order to maximise competition in the supply of systems and components to the commercial benefit of the industry as a whole. In general, it promotes open standards but it does not disallow proprietary solutions where they are offered on reasonable, non-discriminatory, terms and contribute towards the ultimate objective of interoperability.

ITSO has been established to maintain the technical specification and Business Rules required to facilitate interoperability. It also accredits participants and interoperable equipment. ITSO is a facilitator of interoperability at the minimum level of involvement necessary. It will not involve itself in any commercial decisions or arrangements for particular ticketing schemes; neither will it set them up nor run them. It will however "register" them in order to provide the necessary interoperability services (e.g. issue and control of unique scheme identifiers, certification and accreditation, security oversight).

Consequently, adoption of this Specification for particular ticket schemes will be a matter for the commercial judgement of the sponsors/participants, as will the detailed Business Rules and precise partnership arrangements.

Contents

1. Scope	5
1.1 Scope of Part 11.....	5
1.2 Context of a Remote POST within the ITSO Environment	5
2. Remote POST Overview.....	6
2.1 Remote POST Components.....	6
2.1.1 Remote POST Business Logic	6
2.1.2 Remote POST Server.....	6
2.1.3 Customer Media Interface.....	7
2.2 Remote POST Topologies	7
2.3 Remote POST Classes	8
3. Remote POST Interfaces.....	9
3.1 Remote POST Customer Media Interface.....	9
3.1.1 General	9
3.1.2 Platform Support	9
3.2 Remote POST to HOPS Interface.....	9
3.3 Remote POST to ISAM Interface	9
3.3.1 Physical	9
3.4 Human Interface.....	9
3.5 Remote POST Business Logic to Server Interface	10
3.5.1 General	10
3.5.2 Security Considerations	10
3.6 Remote POST Server to CMI Interface	10
3.6.1 General	10
3.6.2 Security Considerations	11
3.7 Audit Trail	11
4. Remote POST Functional Requirements	11
4.1 Media Handling	11
4.1.1 Detection and Validation of the ITSO Shell.....	11
4.1.2 Transaction Time	12
4.2 IPE Handling.....	12

4.3 Message Generation and Processing..... 12

4.4 Configuration Handling 12

4.4.1 Hotlist..... 12

4.4.2 Actionlist..... 12

4.4.3 POST Configuration Data..... 12

1. Scope

ITSO TS 1000 defines the key technical items and interfaces that are required to deliver Interoperability. To this end, the end-to-end security system and ITSO Shell layout are defined in detail while other elements (e.g. terminals, 'back-office' databases) are described only in terms of their interfaces. The Business Rules that supplement the technical requirements are defined elsewhere.

1.1 Scope of Part 11

This part of ITSO TS 1000 defines the requirements on Remote Point of Service Terminals (POSTs) in order that such terminals are able to support the Interoperable Smart Customer Media environment defined by ITSO. These Remote POST requirements are grouped as follows.

- Remote POST Overview
- Remote POST Interfaces
- Remote POST Functional Requirements

Only requirements that are pertinent to Interoperable Smart Customer Media usage and interfacing to other parts of the ITSO Environment are defined herein. These requirements shall be applied as an Interoperability layer over the basic specification of a web or LAN based ticketing solution. The overall specification of such a solution is outside the scope of this document.

For the avoidance of doubt, the fact that a Remote POST may be certified as ITSO compliant does not mean that it is fit for purpose in any area other than its support for Interoperable Smart Customer Media usage. The design of any Remote POST shall mitigate all appropriate risks identified within the risk assessments for the environment within which it operates.

1.2 Context of a Remote POST within the ITSO Environment

Within the ITSO Environment, a Remote POST is defined as a POST with the following key differences:

- They shall use ISAM resources on a server that is remote to the device that the user presents their customer media to.
- They shall perform ITSO transaction processing logic on a server that is remote to the device that the user presents their customer media to.

2.1.3 Customer Media Interface

The Customer Media Interface (CMI) is the component of a Remote POST system that performs the communication with the ITSO Customer Media Device (CM). The CMI is a lightweight component which carries out the activities requested by the Remote POST Server. The CMI is responsible for the following functions:

- Polling for and detecting presence of a CM
- Communicating the presence of a CM to the Remote POST Server
- Communicating with a CM as instructed by the Remote POST Server

2.2 Remote POST Topologies

The following Remote POST Topologies are allowed:

- All components separate as shown in Figure 2, i.e. the Remote POST Business Logic is a web retail site hosted on Server A, the Remote POST Server is hosted on Server B and the Customer Media Interface is hosted on a remote host at some other location, e.g. a home computer. (Note that Server A and Server B may or may not be collocated but are physically separate in communications terms.)

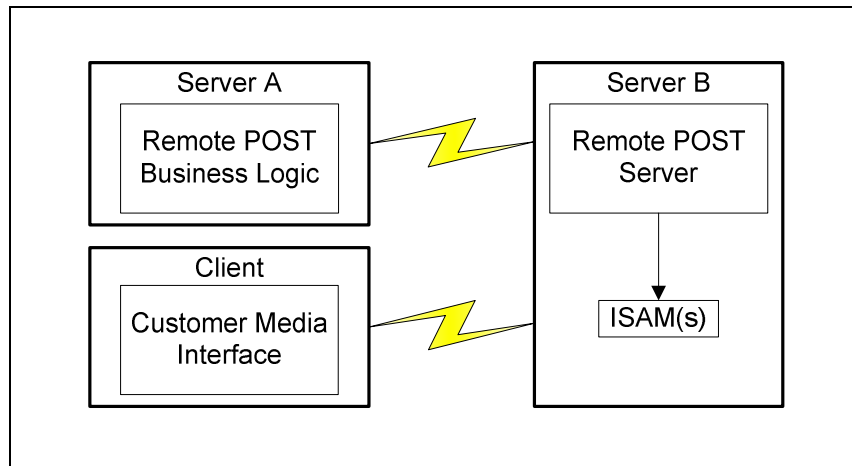


Figure 2 - All Components Separate

- Remote POST Server and Business Logic together as shown in Figure 3, i.e. the Remote POST Business Logic and Server are both hosted on the same Server and the Customer Media Interface is hosted on a remote host at some other location, e.g. a home computer.

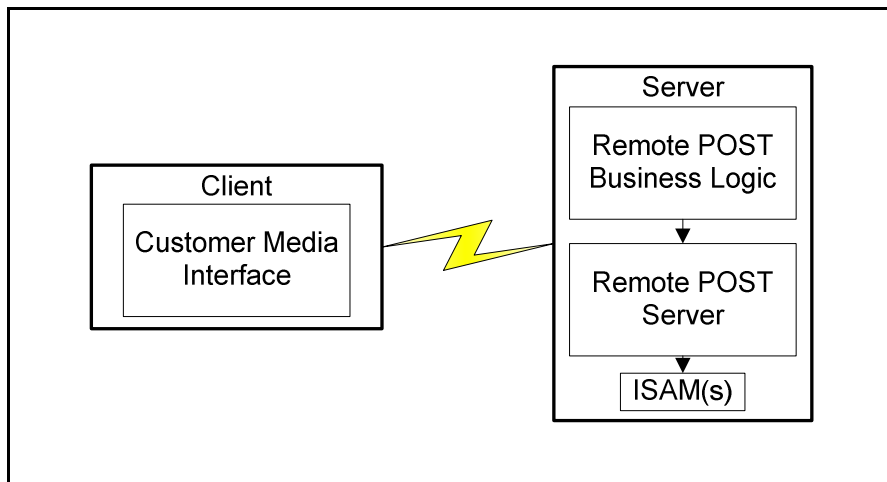


Figure 3 - Remote POST Server and Business Logic Together

- Remote POST Business Logic and Customer Media Interface together as shown in Figure 4, i.e. the Remote POST Server is hosted on Server B, and the Remote POST Business Logic and Customer Media Interface are both co-hosted on a remote host at some other location, e.g. a station ticket machine.

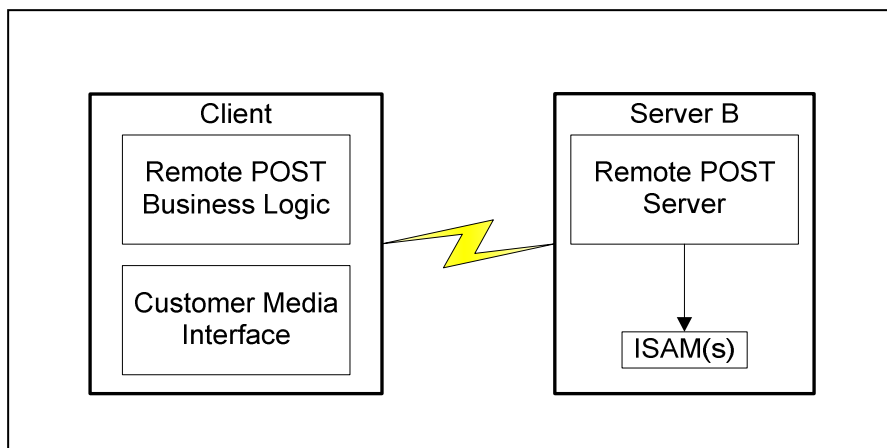


Figure 4 – Remote POST Business Logic and CMI Together

For the avoidance of doubt, when any components are hosted at separate sites their connection may be achieved by any suitably secure means possible, e.g. by Internet, LAN or WAN.

2.3 Remote POST Classes

There are two distinct classes of Remote POST:

- A Public Remote POST is defined as a Remote POST that is available for use by the general public, e.g. a station ticket machine.
- A Private Remote POST is defined as a Remote POST that is only available to a limited user base, e.g. home users, corporate customers, executive club members.

3. Remote POST Interfaces

3.1 Remote POST Customer Media Interface

The Remote POST Customer Media interface is very similar to that of a POST, as defined in ITSO TS 1000-3 Clause 2. The differences are defined in subsequent clauses. This interface is provided by the Customer Media Interface component of a Remote POST.

3.1.1 General

Within the ITSO environment, the primary purpose of a Public Remote POST is to read and write to contactless Customer Media as defined in ITSO TS 1000-3 clause 2.1.

The primary purpose of a Private Remote POST is to read and write to contact or contactless customer media. As such, all Private Remote POSTs shall provide either a contactless interface as defined in ITSO TS 1000-3 clause 2.1, and/or a contact interface that complies with the appropriate parts of ISO/IEC 7816.

If a Private Remote POST only provides a contact interface it is only required to provide a reader that complies with the form factors defined by ISO/IEC 7816-1.

A Private Remote POST implementation with a CMI that is intended for use in the end users home should not be tied to a single customer media interface. E.g. it may support a range of PC/SC (Personal Computer/Smart Card) compliant smart card readers or other smart enabled devices.

3.1.2 Platform Support

A Public Remote POST shall support the entire set of CM platforms as defined in ITSO TS 1000-3 Clause 2.2.

A Private Remote POST is only required to support a subset of the CM platforms defined in ITSO TS 1000-10 based on the following:

- The interface provided, e.g. a Remote POST providing only a contact interface need not support any platform that does not provide a contact interface.
- The business requirements of the system and/or scheme, e.g. a Remote POST that is only designed for use by home users to download IPEs onto media provided to the system users need only support the platforms chosen by the ITSO Licensed Member.
- Security considerations: a Remote POST shall only support CM platforms deemed suitable for use, as defined in the document Developer Guidance CM and remote loading of IPEs, DG0023.

3.2 Remote POST to HOPS Interface

The Remote POST to HOPS interface is identical to that of a POST, as defined in ITSO TS 1000-3 Clause 3.

3.3 Remote POST to ISAM Interface

The Remote POST to ISAM interface is very similar to that of a POST, as defined in ITSO TS 1000-3 Clause 4. The differences are defined in subsequent clauses. This interface is provided by the Remote POST Server component of a Remote POST.

3.3.1 Physical

Every Remote POST Server shall be fitted with at least one ISAM socket or standard contact card reader. The ISAM socket shall accept devices in the ID-000 format; the standard contact card reader shall accept devices in the ID-1 format. Note that ID format is as defined in ISO/IEC 7810.

The socket or contact card reader shall allow the ISAM to be inserted and removed without risk of damage to the ISAM or POST. If the Remote POST Server is located within a physically secured environment with access control, the socket or contact interface is not required to lock the ISAM securely in place and is not required to be located such that tool access is required to access it (as defined in ITSO TS 1000-3, clause 4.2).

3.4 Human Interface

The Human Interface to a Public Remote POST is as defined in ITSO TS 1000-3 Clause 5. The Human Interface to a Private Remote POST is outside the scope of ITSO TS 1000.

3.5 Remote POST Business Logic to Server Interface

3.5.1 General

The Remote POST Server shall allow the Remote POST Business Logic to request some or all of the following operations:

- Creation of one or more products
- Modification of one or more products
- Deletion of one or more products
- Verification and validation of one or more products
- Sending of queries to the HOPS

Any of these operations may be targeted at a specific Shell instance by means of ISRN. For the avoidance of doubt, a Remote POST Server is not required to provide all of these functions; this requirement will be driven by the business needs. The detailed structure of this interface is outside the scope of ITSO TS 1000.

3.5.2 Security Considerations

The Remote POST Server shall only accept requests from Remote POST Business Logic components that have been authenticated and are therefore known. The trust methodology is ultimately the responsibility of the ITSO Licensed Member implementing the remote POST into its scheme and should be based upon appropriate risk analysis. Examples of such trust methodologies include, but are not limited to:

Where the Remote POST Business Logic and Remote POST Server are hosted at different locations:

- Authentication using TLS or SSL where the client and server mutually authenticate.
- Authentication using some form of trusted device, e.g. a SAM.
- Network lockdown utilising a device such as a firewall.

Where the Remote POST Business Logic and Remote POST Server are hosted at the same location:

- Hosting the Remote POST Business Logic and Server at the same site and only allowing local requests.

3.6 Remote POST Server to CMI Interface

3.6.1 General

The Remote POST Server shall allow the CMI to request the continuation of a transaction that was previously requested by the Remote POST Business Logic component. The CMI shall only make this request upon detection of the presence of a single candidate CM. The Remote POST Server shall respond with one or more of the following messages¹:

- Instruction to communicate with the CM
- Notification that the transaction is complete
- Notification that the transaction has failed

The detailed structure of this interface is outside the scope of ITSO TS 1000.

¹ Further messages may be required depending upon the specific implementation

3.6.2 Security Considerations

The Remote POST Server shall accept requests from any CMI component that it wishes; a trust methodology may not be required, because the Customer Media is the trusted component. However, any appropriate trust methodology may be utilised if desired by the ITSO Licensed Member implementing the remote POST into its scheme. Examples of suitable trust methodologies are included in the document Developer Guidance CM and remote loading of IPEs, DG0023.

The Remote POST Server shall ensure that all requests made to the CMI:

- Cannot be read and understood by unauthorised persons, i.e. they are encrypted or obfuscated
- Cannot be intercepted and modified without detection and that if any interception is detected then the Remote POST Server shall abort the transaction, i.e. if any request made by the Remote POST Server has not been carried out then it shall end the transaction.
- Are carried out within a specific time period and that if the request has not been carried out within this time period then the Remote POST Server shall abort the transaction, the time period should be configurable.

3.7 Audit Trail

The audit trail shall ensure that at least one of the following approaches is adopted:

- The customer that performed the transaction can be identified, e.g. a Private Remote POST that involves some form of customer login shall record the customer's details.
- The CMI that performed the transaction can be uniquely identified, e.g. a Public Remote POST CMI must be uniquely identifiable and its identification shall be recorded.

The audit trail shall always contain a record of the following information:

- The date and time at which the transaction was conducted.
- The CM involved in the transaction, i.e. the ISRN of the ITSO Shell.
- The identity of each of the components involved in the transaction, i.e. the Remote POST Business Logic, the Remote POST Server and the CMI (where possible).
- The ISAMID of the ISAM used throughout the transaction.
- ID of IPE(s) used/created/acted upon.
- Nature of the transaction.
- Outcome of the transaction.

4. Remote POST Functional Requirements

The Remote POST functional requirements are largely identical to that of a POST, as defined in ITSO TS 1000-3 Clause 6. The differences are defined in subsequent clauses.

4.1 Media Handling

As defined in ITSO TS 1000-3 Clause 6.1. For a Public Remote POST no differences apply. For a Private Remote POST the differences defined in subsequent clauses apply.

4.1.1 Detection and Validation of the ITSO Shell

As stated in Clause 3.1.1, a Private Remote POST is not required to automatically detect and initiate communications with all Customer Media platforms defined in ITSO TS 1000-10.

4.1.2 Transaction Time

Private Remote POSTs are not required to meet the benchmark transaction times defined in ITSO TS 1000-10. Private Remote POSTs are also not required to maintain an average sustained throughput of 3 transactions per second. Timing and throughput will both depend upon the business requirements and deployment of the system, e.g. a Remote POST that is only designed for use by home users is likely to have extremely relaxed timing and throughput is likely to be irrelevant.

4.2 IPE Handling

As defined in ITSO TS 1000-3 Clause 6.2.

4.3 Message Generation and Processing

As defined in ITSO TS 1000-3 Clause 6.3.

4.4 Configuration Handling

4.4.1 Hotlist

As defined in ITSO TS 1000-3 Clause 6.4.1. Support is mandatory for both a Public and Private Remote POST.

4.4.2 Actionlist

As defined in ITSO TS 1000-3 Clause 6.4.2. Support is mandatory for a Public Remote POST and optional for a Private Remote POST.

4.4.3 POST Configuration Data

As defined in ITSO TS 1000-3 Clause 6.4.3. Support is optional for both a Public and Private Remote POST.