

IOPHub

Data Security Guidelines



Version 1.0
June 21, 2007

The information disclosed herein is ELECTRONIC TRANSACTION CONSULTANTS CONFIDENTIAL and PROPRIETARY and intended for NTTA, HCTRA CTRMA and TTA internal distribution only. Neither this document nor the information disclosed herein shall be reproduced or transferred to other documents or used or disclosed to others except as specifically authorized by Electronic Transaction Consultants.



1705 North Plano Road, Richardson, TX 75081
Ph: 214-615-2302, Fax: 214-615-5001, Website: www.etcc.com



IOPHub Data Security Guidelines

Revision History

Author	Revision Date	Revision #	Reason for Change
Vincent Zontini	11/16/2006	0.6	Initial Draft
ETC	06/21/2007	1.0	Updated w. IOPHub cover page, header & footer; standardized terms.

Table of Contents

Revision History	ii
Table of Contents	ii
IOPHub Data Security Guidelines	1
Introduction.....	1
Connectivity Description	2
IOPHub Block Diagram.....	3
Policies	4
Security Review.....	4
Written Connectivity Agreement	4
Point Of Contact.....	4
Connectivity Guidelines	4
Minimum Standards	5
Desired Standards	5
Modifying or Changing Connectivity and Access.....	5
Terminating Access.....	6



IOPHub Data Security Guidelines

IOPHub Data Security Guidelines

Introduction

The IOPHub (or “interoperability hub”; formerly known as SmartHub) solution for interoperability utilizes a Service-Oriented Architecture (SOA) to exchange information efficiently and reliably between participating agencies. Within the IOPHub architecture, a Service Provider is an Authority that operates and maintains a customer service center that issues AVI transponders for electronic payment of AVI transactions, such as toll road fees (tolls) and parking fees. A Subscriber is an Authority that employs a service provider to conduct customer service center operations. The subscriber Authority does not maintain its own customer accounts, nor operate its own customer service center. For the purposes of this document both Service Providers and Subscribers will be referred to simply as Authorities. The IOPHub itself is the component of the solution that processes and distributes shared interoperability information between the Authority layers. The IOPHub will be implemented with two locations to provide disaster recovery.

The interconnected nature of the IOPHub information system requires that all Authorities use a standard method of interconnecting with the IOPHub information system and observe a minimum level of security. This document defines the minimum level of due care. As a condition of continued access and use, all participating Authorities and their employees must observe the requirements and procedures set forth in this document.

The IOPHub is designed to be independent of the Authorities. Also the IOPHub hosting organization (IHO) for the IOPHub primary and standby sites can be different. Private network connections between member Authorities and IOPHub that pass through non-public IHO resources fall under this policy, regardless of whether a telephone company circuit (such as frame relay or ISDN) or virtual private network (VPN) technology is used for the connection.



IOPHub Data Security Guidelines

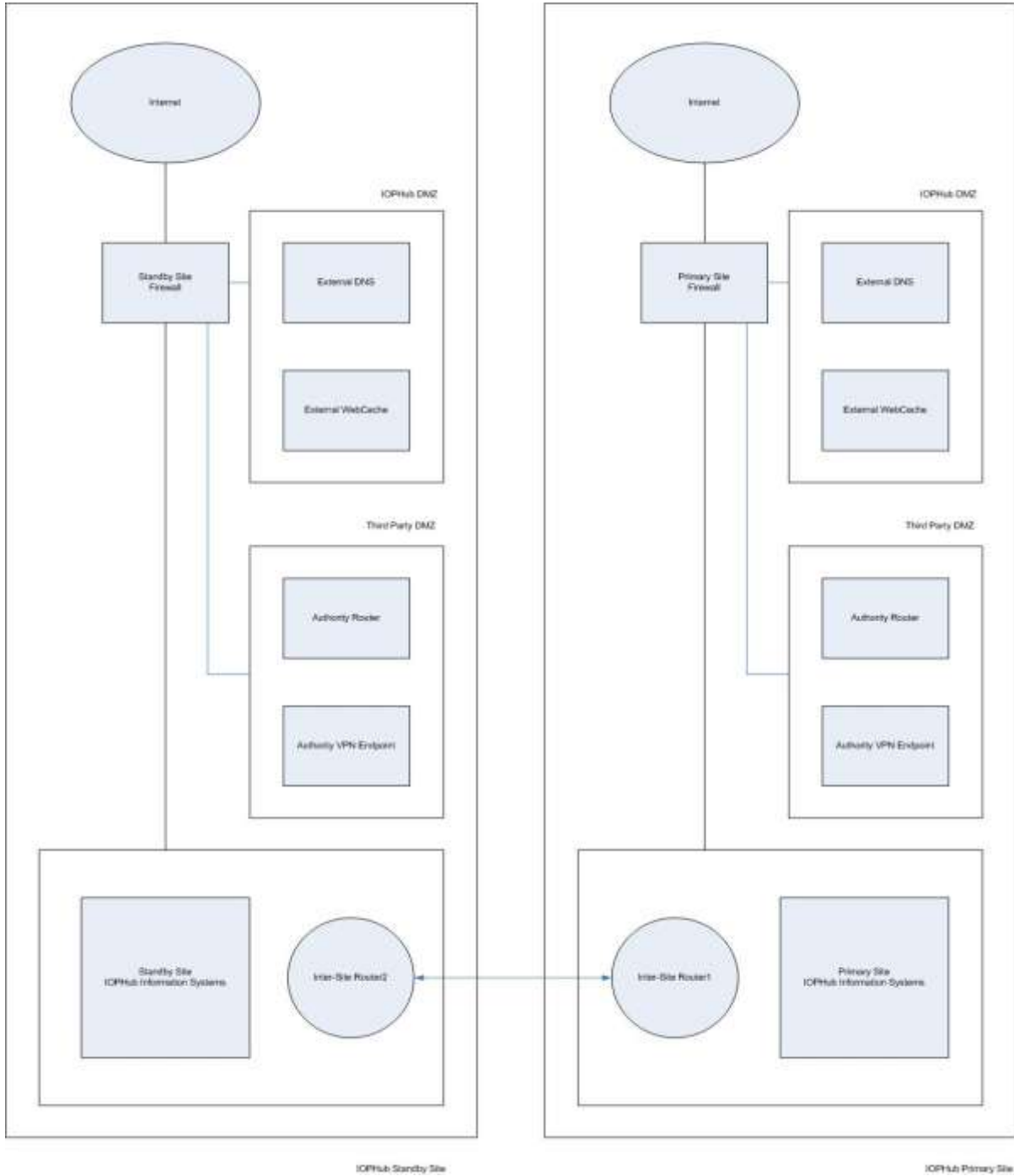
Connectivity Description

HCTRA is currently the IHO for both the primary and standby IOPHub installations. The IOPHub systems are hosted at two separate HCTRA facilities in Houston and require network access to these facilities for Authorities to access the IOPHub. Connectivity to the IOPHub services is made via two paths. The first path is internet access to IOPHub's SSL secured (HTTPS) website at www.iophub.com. The second path is via private network connections between the Authority and IOPHub via the hosting organization's third party DMZ. If an Authority desires to take advantage of the redundant datacenters then private network connectivity must be established to both sites. Therefore in the event that the standby IOPHub site is promoted to primary, the Authority will retain connectivity to the IOPHub systems.



IOPHub Data Security Guidelines

IOPHub Block Diagram





IOPHub Data Security Guidelines

Policies

Security Review

All new connection requests will go through a security review with the IHO's Information Technology (IT) department. The reviews are to ensure that all access meets or exceeds the business requirements in a best possible way and that the principle of least access is followed.

Written Connectivity Agreement

All new connection requests require that the Authority and the IHO agree to and sign a written connectivity agreement. This agreement must be signed by a representative from the Authority who is legally empowered to sign on behalf of the Authority. Executed documents will be kept on file by the IHO IT department.

Point Of Contact

The connection request must designate a person (or list of persons) to be the Point of Contact (POC) for the network connection. The POC acts on behalf of the Authority, and is responsible for those portions of this policy and the connection agreement that pertain to it. In the event that the POC changes the IHO must be informed promptly. The IHO will provide a POC to Authorities for network connectivity and security issues.

Connectivity Guidelines

All connectivity established must be based on the least-access principle, in accordance with the Interoperability Business Requirements. For example, network traffic is to be restricted to only the hosts that need to communicate with each other as well as the specific application ports that are required to those hosts. The traffic restrictions for dedicated lines also apply to VPN connections. The VPN equipment should be at least VPNC Basic Interop Certified. Cisco equipment is preferred. VPN equipment should support IPSEC tunnels, IPsec Encapsulation Security Payload, 3DES or AES with MD5 or SHA.

The IHO will not rely upon the Authority to protect the IOPHub network or resources. As a condition of gaining access to the IOPHub computer network, every Authority must secure its own connected systems in a manner consistent with the Interoperability Business Requirements. The IHO reserves the right to audit the security measures in effect on IOPHub connected systems. The IHO reserves the right to immediately terminate network connections not meeting minimum standards.



IOPHub Data Security Guidelines

Minimum Standards

A written password policy meeting at least the following standards must be available: a minimum password length of 8 characters, minimum password strength of one upper case, one lower case, and one non-alphabet character, and maximum password age of 90 days. No system or software default passwords are allowed.

The Authority must be able to demonstrate that their network is properly protected from the internet and other networks via firewalls, router access lists, or other applicable technology.

The Authority must be able to demonstrate that physical security measures are in place for the equipment supporting the connectivity with IOPHub. For example the computer and network equipment must be stored in a locked room that can only be accessed by authorized persons.

The Authority must be able to demonstrate that network access control measures are in place for the network supporting the connectivity with IOPHub. For example, a written policy is in place detailing the restrictions on new computer connections to the network, remote network access, and/or wireless access to the connecting organizations network.

The Authority must be able to demonstrate a policy that anti-virus software is installed, current and actively running on all systems commonly affected by viruses, especially personal computers and servers. This policy does not include UNIX-based operating systems or mainframes.

The Authority must agree to network vulnerability scans. The IOH will notify the organization that a scan has taken place; however, due to the nature of these scans the IOH may not provide advance notice.

Desired Standards

The security standards that are most desirable are the ones provided in the latest version of the Payment Card Industry (PCI) Data Security Standards (DSS) as published by PCI Security Standards Council at <https://www.pcisecuritystandards.org>.

Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Authority is responsible for notifying the IHO



IOPHub Data Security Guidelines

when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

Terminating Access

When access is no longer required, the Authority must notify the IHO IT team which will then terminate the access. The IHO IT security teams will conduct an audit of external connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct IOPHub business, will be terminated immediately. Should a security incident or a finding that a circuit has been depreciated and is no longer being used to conduct IOPHub business necessitate a modification of existing permissions, or termination of connectivity, the IHO IT team will do its best to notify the POC of the change prior to taking any action.