

INFINITY

Automated Call Distribution
and
Unified Messaging System

HIPAA READINESS DISCLOSURE

Publication © 2006

1CALL

a division of

amtelco

4800 Curtin Drive, McFarland, Wisconsin USA 53558-9424
www.1Call.com

American Tel-A-Systems Inc.

Infinity HIPAA Readiness Disclosure

Amtelco publication © American Tel-A-Systems, Inc., June 2001. All rights reserved.

Amtelco Documentation

This document and the information contained herein are proprietary to American Tel-A-Systems, Inc. It is provided and accepted in confidence only for use in the installation, training, operation, maintenance, and repair of Amtelco equipment by the original owner. It also may be used for evaluation purposes if submitted with the prospect of purchase of equipment.

This document is not transferable. No part of this document may be reproduced in whole or in part by any means, including chemical, electronic, digital, xerographic, facsimile, recording, or other method, without the expressed, written, permission of American Tel-A-Systems, Inc.

Amtelco offers a number of proprietary manuals describing the functions and features of its product lines. Further information and instructions concerning topics included in this publication can be found in several of Amtelco documents. If you do not have these documents on hand, contact Amtelco Telemarketing at 1-800-356-9148 between 8 a.m. and 5 p.m., Central Time.

Trademarks and Copyrights

Amtelco and Infinity are federally registered trademarks of American Tel-A-Systems, Inc., and are covered and protected by one or more of the following United States patents: 4,916,726; 5,113,429; 5,259,024; 5,469,491; 6,141,413. Other patents, both foreign and domestic, are pending.

The following statement is made in lieu of using a trademark symbol with every occurrence of registered, trademarked and copyrighted names:

Registered, trademarked and copyrighted names are used in this document only in an editorial fashion, and to the benefit of the registration, trademark or copyright owner with no intention, expressed or implied, of infringement of the registration, trademark or copyright.



American Tel-A-Systems Inc.
4800 Curtin Drive, McFarland, Wisconsin USA 53558-9424

Visit Amtelco on the World Wide Web at <http://www.amtelco.com>

Table of Contents

Executive Summary.....	1
Corporate Profile	1
HIPAA Compliancy.....	1
System Integrity.....	1
System Configuration.....	1
Applications Security.....	2
HL7 Compatibility.....	2
Software Platform	3
Software Configuration	3
Software Expansion	3
Software Improvement.....	3
Software Platform	3
Infinity Configuration.....	4
Network Security.....	5
Telephone Interconnectivity.....	5
Network Configuration.....	5
Network Security.....	5
CTI Server Security.....	6
CTI Server Configuration.....	6
Server Console	6
Server Security.....	6
Remote CTI Server Access	6
Remote Diagnostics Modem.....	7
Alphanumeric Paging / Remote Message Delivery Modems	8
CTI Server Backup.....	8
Software Applications Security	9
Infinity Applications Security	9
Windows Security.....	9
Infinity Applications Access	11
Infinity Telephone Agent.....	11
Infinity Supervisor	11
Operator / Supervisor Set-up	12
User Access Levels.....	12
Client Data Security.....	13
Client Account Database.....	13
Client Account Security.....	13
Information Compatibility.....	14
HL7 Compatibility.....	14
Web Access Security.....	15
Web Application Configuration	15
Web Application Security	15
Hosted Web Services.....	16
Telephone Connectivity	16
Internet Connectivity.....	16
System Reliability.....	16
System Security.....	17

Corporate Profile

Amtelco is a manufacturer and distributor of computer telephony integration (CTI) based call distribution and messaging equipment for healthcare facilities, universities, telephone answering services, executive suites, contact centers and corporations. Amtelco has been a trusted name in the call center industry for three decades. Thousands of Amtelco systems and computer components have been installed in all 50 of the United States, Australia, Canada, Chile, Columbia, England, Mexico, the Netherlands, Puerto Rico, and the U.S. Virgin Islands.

The Amtelco Infinity automated call distribution and unified messaging system is installed in facilities where it is connected to the telephone network and often to an existing data network. It is imperative that the Infinity system be secure from unauthorized access. This document describes the HIPAA readiness status of the Infinity system. Each of the several elements that combine to make Infinity a highly secure system is discussed in detail in the following pages.

Commitment to HIPAA Compliancy

The Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, is an element of the healthcare reform package enacted by Congress in 1996. All hospitals and clinics are expected to be HIPAA compliant, by April 2004.

The advent of HIPAA has sparked far-reaching changes in the ways the healthcare industry conducts its business. The 1Call division of Amtelco is committed to assisting its customers in the healthcare fields in their efforts to achieve compliance with the HIPAA standards.

Amtelco has empanelled a working group to monitor the development of the HIPAA standards and to direct Amtelco's on-going efforts to ensure that all Amtelco software applications and hardware installations conform to the security policies required by HIPAA as these standards are developed.

This interdepartmental effort is comprised of the director of software research and development, the manager of quality control and assurance, the manager of corporate management information services, the products and applications manager of the 1Call healthcare marketing division and the senior software documentation editor.

System Integrity

The information as stated in these pages is applicable to the hardware, operating system and database of the Infinity system in its configuration at the time of installation. Changes made by persons other than those under the employ, consult or direct instruction of Amtelco may compromise the stated measures or integrity of system security. Amtelco cannot assume responsibility for the loss, theft or alteration of data within the Infinity system following the transfer of ownership and control of the system to the customer named in the contract of sale.

System Configuration

The Infinity automated call handling and unified messaging system is intended for secure and specific limited access. Though the system is designed to run continually, 24 hours a day, seven days a week, access is controlled by a secure, hard-coded log-in procedure.

Executive Summary

The Infinity system is designed to operate as an Ethernet Local Area Network (LAN) running the Microsoft Windows 95/98/NT operating system. The Infinity LAN connects the Infinity CTI server with the supervisor and agent workstations and all Infinity applications resident on the workstations. The Infinity LAN can be connected to an existing on-site data network using the TCP/IP protocol.

System security is enhanced by elements of the hardware configuration and the software license agreement that specify the number and types of workstations that can be included in the system and that can be loaded with and operate on the Infinity software.

The Infinity CTI Server can provide interfaces to one or more telephony networks. These can include analog and digital telephony trunks from the local central office as well as short haul and on-premise connections to other PBX and call switching equipment.

Applications Security

All Infinity applications are constructed on the Microsoft Windows 95/98/NT platform. This enables the incorporation of all the security and functionalities of the Windows operating system into the Infinity applications, including, but not limited to, encryption, usage logging and user access.

The Infinity system is designed to operate as an Ethernet Local Area Network (LAN) running the Microsoft Windows 95/98/NT operating system. The Infinity LAN connects the Infinity CTI server with the supervisor and agent workstations and all applications resident on the workstations.

Security was included as part of the initial design specifications for the Windows NT version of the platform and is pervasive throughout the implemented operating system. All Amtelco applications conform to the Windows NT security model.

HL7 Compatibility

The Infinity automated call handling and unified messaging system supports an interface to existing healthcare information systems to receive real-time patient Admission, Discharge and Transfer (ADT) information using the Hospital Level 7 (HL7) protocol.

The HL7 interface is used to populate listings in the Infinity CTI server directory. Directory listings can be used by operators to transfer calls to patient rooms, to provide callers with patient information, and to accomplish other tasks dependant on data in the HL7 record.

Disclaimer

Amtelco has made, and continues to make, every reasonable and prudent effort to provide and maintain an acceptable level of security for the software and customer-provided data within the Infinity Computer Telephony Integration (CTI) Server. Although the following measures attempt to address the means of access to the database and operating system of the Infinity Computer Telephony Integration Server, known or possible to the best of Amtelco's knowledge, this document cannot provide a guarantee, either expressed or implied, against unauthorized access to the information contained within the Infinity Computer Telephony Integration Server.

Software Configuration

The Infinity automated call distribution and unified messaging system is, at its heart, a software platform comprised of three specialized applications, each with its own security and access restrictions:

The Infinity Host CTI server application runs on a dedicated chassis and performs automated call handling and unified messaging tasks. Access to the Infinity CTI server operating system is permissible only at the Infinity server console and is password protected.

The Infinity Supervisor workstation application is installed on a limited number of desktop computer workstations and is used to set up and maintain the system configuration, to assign user access and to set up and maintain the database of client accounts. Access to individual supervisor workstations is password protected. Access to the Infinity CTI server operating system is unavailable at supervisor workstations.

The Infinity Telephone Agent workstation application runs on a license-restricted number of desktop computer workstations and is used to perform operator functions and messaging tasks. Access to individual agent workstations is password protected. Access to the Infinity CTI server operating system is unavailable at agent workstations.

Software Expansion

A number of optional and enhanced Infinity software modules that provide additional functionalities are available as separate pay features. Certain of these applications must run on a dedicated desktop computer workstation connected to the Infinity CTI server by way of a serial interface. Some of these applications require a dedicated desktop computer workstation in the system configuration connected to the Infinity CTI server by way of an Ethernet LAN. Others can be installed concurrently with the agent and supervisor applications. Still others can be installed on workstations that are connected to the existing data network in an existing, on-premise LAN

Software Improvement

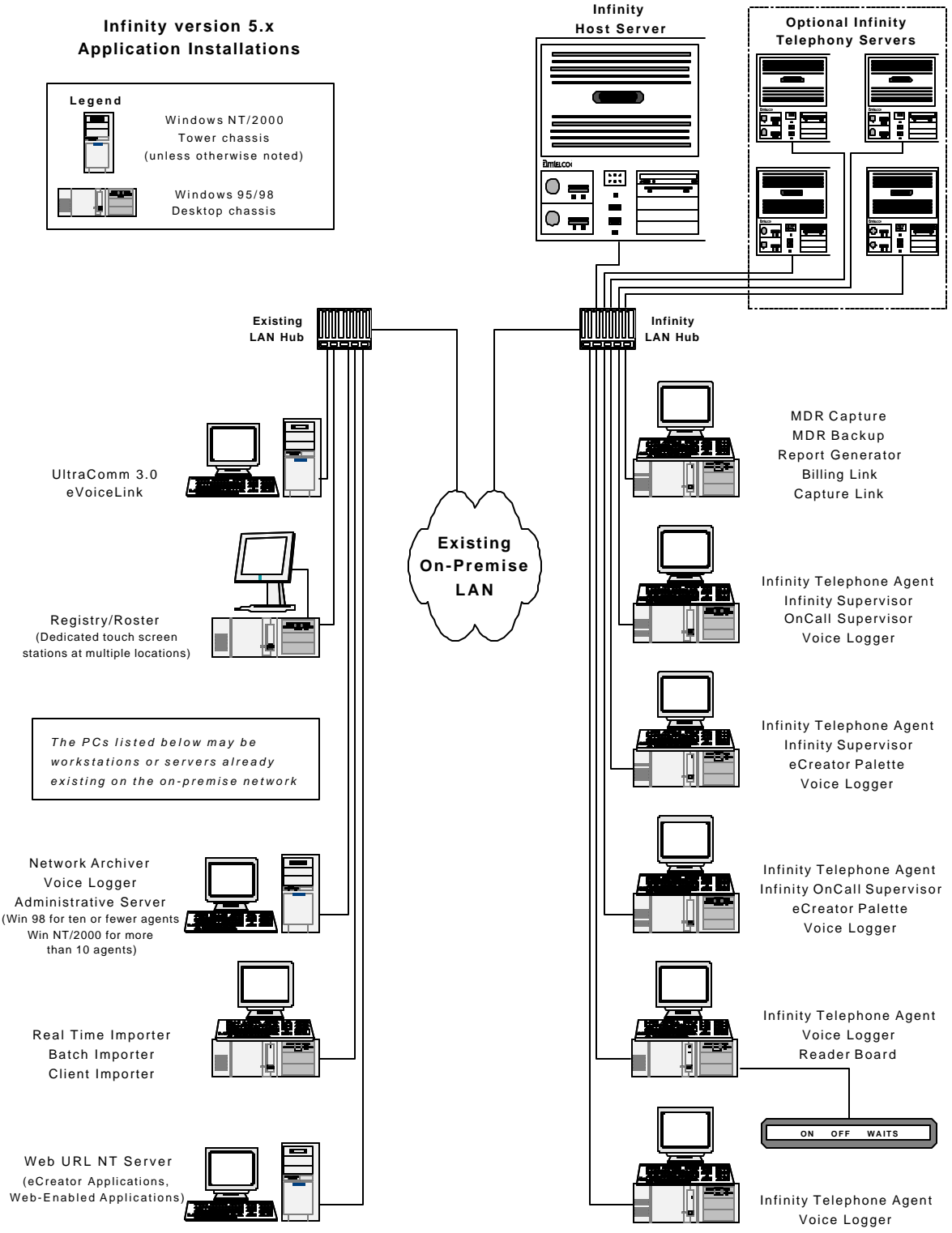
Successive versions of the Infinity software possess individual limits as to the number of available log-in keys and the number of desktop computer workstations that can be included in the system configuration.

Software version	Maximum workstations	Available log-in keys
Infinity 4.x	50	500
Infinity 5.x single CTI chassis	100	2000
Infinity 5.x maximum 5 CTI chassis	100	2000

Software Platform

All Infinity applications are constructed on the Microsoft Windows 95/98/NT platform. This enables the incorporation of all the security and functionalities of the Windows operating system into the Infinity applications, including, but not limited to, encryption, usage logging and user access.

Infinity Configuration



Telephone Interconnectivity

The Infinity CTI Server can provide interfaces to one or more telephony networks. These can include analog and digital telephony trunks from the local central office as well as short haul and on-premise connections to other PBX and call switching equipment.

The majority of these trunks interface to one or more telephony switching cards within the CTI server. All voice and data being brought into these boards from external trunk lines are switched among the boards on a separate digital bus that is dedicated for this purpose. These connections are electrically separated from the ISA or PCI computer bus within the server, and therefore cannot communicate with or affect the database or operating system of the server.

With exception of the telephony switching cards mentioned above, the only remaining connections between the telephone network and the Infinity CTI server take place through the external modems connected to the server. These modems include a remote diagnostic modem as well as one or more modems that are used for alphanumeric paging and remote message delivery.

Network Configuration

The Infinity system is designed to operate as an Ethernet Local Area Network (LAN) running the Microsoft Windows 95/98/NT operating system. The Infinity LAN connects the Infinity CTI server with the supervisor and agent workstations and all applications resident on the workstations.

The Infinity LAN uses the TCP/IP protocol and can be configured for either 10BaseT or 100BaseT connectivity. The Infinity LAN can be connected to an existing on-site data network using the TCP/IP protocol.

The built-in security features of the Windows operating system serve to enhance the levels of security that can be established for access to the Infinity system.

Network Security

The following security statements apply to the Infinity Ethernet LAN.

- ❖ Connection to the Infinity CTI server application is allowed only after entering a valid Login ID. Infinity utilizes a multi-character Login ID plus an optional numeric Passcode to establish a network session with the Infinity CTI server application.
- ❖ The Infinity CTI server application utilizes a proprietary command set based on either the TCP/IP protocol. Invalid commands sent to the Infinity CTI server application are ignored.
- ❖ The proprietary command set of the Infinity CTI server application is available only to a network session after the session has successfully logged into the server.
- ❖ The Infinity CTI server does not support Telnet session connections. A request to connect to the Infinity CTI server application as a Telnet session is ignored.

CTI Server Configuration

The Infinity automated call distribution and unified messaging system can be configured to incorporate from one to five dedicated server chassis. The Infinity Host application runs on the Infinity CTI server a chassis and performs automated call handling and unified messaging tasks. Access to the Infinity CTI server operating system is permissible only at the Infinity CTI server console and is password protected.

Server Console

The Infinity CTI server accommodates connection of a standard 101-key PC keyboard and VGA as a console to monitor the server chassis. The keyboard and monitor are used to view and control the server activity upon initial boot-up, as well as to monitor the state of the various telephony ports once the server is on-line.

In a proper configuration, the server keyboard and monitor do not need to be accessible for the Infinity CTI server to reset or to come on-line. Amtelco does not recommend disconnection of the server keyboard or monitor due to their necessity as diagnostic tools. It is recommended that the server keyboard and monitor be kept near the server and be accessible only to appropriate personnel.

The Infinity CTI server keyboard and monitor have a limited vocabulary of functions they are able to perform. Attempts to execute functions outside of the vocabulary are ignored.

Access to other network devices or computers is not available through the Infinity CTI server keyboard and monitor.

Server Security

The following security statements apply to the Infinity CTI server.

- ✘ Connection to the Infinity CTI server application is allowed only after entering a valid Login ID. Infinity utilizes a multi-character Login ID plus an optional numeric Passcode to establish a network session with the Infinity CTI server application.
- ✘ The proprietary command set of the Infinity CTI server application is a limited vocabulary of commands that only allows execution of pre-determined functions or commands.
- ✘ A log file can be maintained within the Infinity CTI server that records the time and date of each successful user log-in over a given time period as well as the duration of the session before the user logs out.

Server Backup

As an added measure of security, the Infinity CTI server is equipped with a Digital Cassette Tape Drive to allow creation of backup copies of the Infinity database that can be kept off premise. In the event of loss, theft or corruption of data, a backup tape can be used to restore all system software and user data to the state it was in at the point the tape was made.

The data contained on an Infinity Backup Tape is written in a proprietary format. Only the Infinity CTI application is able to decode and utilize the data contained on the tape.

Daily backup tapes, stored in a safe location, provide the ability to restore the system and data to a given state from within the previous twenty-four hours.

Remote CTI Server Access

Remote access to the Infinity CTI server is available on a limited and extremely controlled basis. Remote access through a highly secure remote diagnostic modem that is hard-wired to the Infinity CTI server is required. Additional remote access may be made available for alphanumeric paging and message delivery modems connected to the Infinity CTI server through a serial interface.

Alphanumeric Paging / Remote Message Delivery Modems

Amtelco may connect one or more external modems to an RS-232 serial interface board in the Infinity CTI Server. These modems are used to deliver outgoing alphanumeric pages as well as to accommodate incoming dial-up connections for remote text message delivery.

The following statements apply to the paging and remote message delivery modems.

- ❖ Access to the Remote Diagnostics functions cannot be gained through any modem other than the modem connected to the Remote Diagnostics Port. Diagnostic commands transmitted into alphanumeric or remote-printing modems are ignored.
- ❖ Access to the Infinity CTI Server operating system through the RS-232 alphanumeric paging ports or remote message delivery ports is not available.
- ❖ Remote access to messages contained within individual Client Accounts can be accommodated through dialing into alphanumeric paging modems on the Infinity CTI Server. These remote dial-up connections require both a valid Client Account number and an optional Client Passcode for the user to view messages.

Remote Diagnostic Modem

Amtelco always connects an external modem to the Remote Diagnostics Port, COM Port 2, of the Infinity CTI Server. This modem is used to provide remote diagnostics capabilities for Amtelco Help Desk and Field Engineering personnel.

The following security statements apply to the Remote Diagnostics Port.

- ❖ Amtelco uses an external remote diagnostics modem to allow the modem to optionally be turned off while not in use. If the modem is turned off, Amtelco will instruct on-premise staff to turn on the modem when access is required. After remote diagnostics are complete, Amtelco will instruct on-premise staff to turn off the modem.
- ❖ Amtelco requires that a dedicated phone line be connected to the remote diagnostics modem.
- ❖ Amtelco strongly recommends that the dedicated phone line connected to the remote diagnostics modem have a non-published telephone number.
- ❖ Amtelco utilizes a multi-character Security Passcode to gain access to the Remote Diagnostics Port of the Infinity CTI Server. The Security Passcode is provided only to Amtelco technical staff. The Security Passcode is changed on a regular basis.

CTI Server Security

- ✘ Access to the Remote Diagnostics functions is not allowed without proper entry of the Security Passcode.
- ✘ A log of all Remote Diagnostic Port accesses is kept and can be reviewed from the Infinity Supervisor application.
- ✘ An Infinity System Alarm can be enabled to activate any time a technician or caller enters an invalid Security Passcode. This alarm immediately alerts the call center staff that a possible invalid access was attempted.
- ✘ An Infinity System Alarm can be enabled to activate any time a technician successfully logs into the Remote Diagnostics Port with a valid Security Passcode. This immediately alerts the call center staff that a technician has logged into the Remote Diagnostic Port.
- ✘ After proper entry of the Security Passcode, a technician has limited access to only the vocabulary of Remote Diagnostic Port functions that is built into the Infinity CTI Server application.
- ✘ Access to the Infinity CTI Server operating system through the Remote Diagnostic Port is not available.
- ✘ Access to other network devices or computers through the Remote Diagnostics Port is not available.

Infinity Applications Security

All Infinity applications are constructed on the Microsoft Windows 95/98/NT platform. This enables the incorporation of all the security and functionalities of the Windows operating system into the Infinity applications, including, but not limited to, encryption, usage logging and user access.

The Infinity system is designed to operate as an Ethernet Local Area Network (LAN) running the Microsoft Windows 95/98/NT operating system. The Infinity LAN connects the Infinity CTI server with the supervisor and agent workstations and all applications resident on the workstations.

Security was included as part of the initial design specifications for the Windows NT version of the platform and is pervasive throughout the implemented operating system. All Amtelco applications conform to the Windows NT security model.

Windows Security

The Windows NT security model includes components to control access to each object, such as files and shared printers. It also includes components to control which actions an individual can perform on an object and which events are audited. The Windows NT security model also includes several features designed to grant permissions to some groups of users while denying those permissions to others.

Windows NT and Windows 98 share many of the same security technologies, particularly the Internet-related security technologies. The chief way that they differ is in Windows NT's absolute, from-the-ground-up internal security features, which incorporate a myriad of low-level security checks at every point where objects can be accessed within the operating system.

Although Windows 98 does not implement built-in security anywhere near the level included in Windows NT, a number of security-related features were added or improved upon from Windows 95.

Microsoft has made a thorough discussion of the security readiness, structure and features of the Windows platform available from a number of sources. The following material only serves to summarize the elements of Windows NT security model.

User Accounts – The key to Windows NT security is the availability of user accounts. User accounts can be created as needed. A user account can be included in as many groups of accounts as is appropriate. Access to any computer resource can be permitted or denied to individual accounts or to groups of accounts.

Passwords – The built-in security capabilities include a number of workstation and server password enforcement options. These include minimum password length, minimum and maximum password age, how often a password can be reused and controls over whether a user can, or must, change a password and establishing a maximum number of unsuccessful attempts to log on before an account is locked.

File and Directory Protection – A range of file protections can be set on a per-file or per-directory basis. These protections can be assigned on a per-user or per-group basis. Security checks are then performed automatically when files are accessed.

Registry Protection – The registry of a computer is the repository of all system configuration information. Security against unauthorized access to and alteration of the registry is essential, but users and applications that need to access or alter registry information must be allowed to do so. A specialized registry editor application is included in the operating system for this purpose.

Printer Protection – Specific users can be allowed to or prevented from printing to a system or networked printer. This permission can even be refined to encompass all or only part of the workday.

Auditing – A built-in auditing capability enables tracking to determine which user account was used to attempt what kind of access to files or other objects. Auditing also can be used to track log-on attempts, system shutdowns or restarts, and similar events.

Secure Channels – Built-in support for secure channels includes the Point to Point Tunneling Protocol (PPTP), which enables users to connect securely to a remote network, even over an intervening insecure network if necessary. This is accomplished by means of encrypted encapsulated packets and enables one protocol to be nested inside another. Thus, a user can connect, for example, to the Internet via TCP/IP, then establish a secure IPX connection to another network. Support for Secure Socket Layer (SSL) has been upgraded, which increases the level of encryption that can be applied to Internet and intranet data exchanges.

Smart Cards – Built-in support for smart cards consists of a two-layer driver model designed to encompass smart card reader hardware, together with the APIs used to authenticate, write to, and retrieve data from smart cards. These cards have at least three important uses: as user authentication in place of or in addition to log-on sequences, for transacting financial business over the Internet and elsewhere, and as portable data repositories for storing bits of information such as one's drug allergies or dental history.

Credit Card Protection – Crypto API, Authenticode and Microsoft Wallet support first appeared as part of Internet Explorer (IE) in version 4.0 and are still included with its subsequent versions.

Windows Built-in Security Technologies by Version

Technology	Win 95	Win 98	Win NT
Group-level security	Partial	Partial	Yes
File-level security	No	No	Yes
Object rights and privileges	No	No	Yes
PPTP client	Add-on	Yes	Yes
PPTP server	No	Yes	Yes
Smart cards	Add-on	Yes	Yes
Crypto API	Add-on (IE4)	Yes	Yes
Authenticode	Add-on (IE4)	Yes	Yes
Microsoft Wallet	Add-on (IE4)	Yes	Yes

Infinity Applications Access

The Infinity automated call handling and unified messaging system is intended for secure and specific limited access at user workstations connected to the Infinity CTI server in an Ethernet LAN. Though the system is designed to run continually, 24 hours a day, seven days a week, access is controlled by a secure, hard-coded log-in procedure.

The log-in procedure in all Infinity applications can be configured to require that each user enter either one or two pre-assigned alphanumeric keys before access to the system is granted. The availability of only a limited number of user log-in keys serves to enhance system security. Successive versions of the Infinity software possess individual limits as to the number of available log-in keys.

Assigning unique, user-specific levels of access for each individual who is authorized for access can further enhance system security.

Infinity Telephone Agent

The Infinity Telephone Agent call-handling and messaging software is designed to run 24 hours a day, seven days a week, throughout all operator work shifts. Individuals are required to log in and log out as they begin and end their shifts. When the software is running and no one is logged in at an agent workstation, the Infinity Telephone Agent Login Prompt is displayed with the cursor blinking in the Login Name field.

A Login Name and, if desired, an optional Password, are required to log in as an Infinity operator. This verifies to the Infinity CTI server that an individual is authorized to perform Infinity Telephone Agent commands. An individual cannot be logged in as a supervisor and an operator under the same Login Name at the same time.

When the system is first install and no other Login names are set up, the pre-configured Login Name *System* allows access to the Infinity Telephone Agent software.

Among the first tasks that should be performed after installation of the system, it is suggested that a confidential *Access Code* be assigned to the *System* Login Name to prevent its subsequent unauthorized use.

Infinity Supervisor

The Infinity Supervisor system management is designed to be run as needed, though it can be left running 24 hours a day, seven days a week. Individuals are required to log in and log out as they begin and end their supervisory tasks. When the software is running and no one is logged in at a supervisor workstation, the Infinity Supervisor Login Prompt is displayed with the cursor blinking in the Login Name field.

A Login Name and, if desired, an optional Password, are required to log in as an Infinity supervisor. This verifies to the Infinity CTI server that an individual is authorized to perform Infinity Supervisor commands. An individual cannot be logged in as a supervisor and an operator under the same Login Name at the same time.

When the system is first install and no other Login names are set up, the pre-configured Login Name *System* allows access to the Infinity Supervisor software.

Among the first tasks that should be performed after installation of the system, it is suggested that a confidential *Access Code* be assigned to the *System Login Name* to prevent its subsequent unauthorized use.

Operator/Supervisor Set-up

Creating an Infinity supervisor or operator identity consists of establishing a *Login Name* and assigning various features related to call handling and other tasks, including:

- ✘ An optional *Access Code* for additional security
- ✘ Limiting the number of calls on screen at one time
- ✘ Assigning calls to specific client accounts to specific operators
- ✘ Establishing access to Infinity Supervisor commands, stations, and data including a range of supervisory security levels
- ✘ Enabling a beeping alarm at the arrival of each new call
- ✘ Setting an *Operator Greeting Number*, part of the optional *Perfect Answer* feature, which allows an operator to record a greeting for each client that is played automatically when the operator answers a call for that client.

User Access Levels

Specific levels of access can be assigned to each individual authorized to use the Infinity Telephone Agent and Infinity Supervisor software applications.

The Operator Set-up screens include *Access Enabled* and *Access Disabled* menus, which regulate an individual's access to the entire range of Infinity commands, software features and system data.

When a feature is enabled in the *Access Enabled* menu, that individual can perform all the tasks, and Infinity will accept all the commands, relating to that feature. Any feature listed in the *Access Disabled* menu cannot be accessed by that individual.

The *Access Enabled* features control the Infinity system options, and allow access to reports covering clients, operators, supervisors, the system and call traffic. It may prove best to start an individual with minimal access and add permissions as that individual gains experience and proves dependability.

Client Account Database

The client account database is the backbone of the Infinity automated call distribution and unified messaging system. Each user is assigned a unique client account number in the database that identifies the user to the Infinity CTI server. All call distribution, messaging and reporting functions are performed by the Infinity CTI server according to the parameters established when a client account is created in the database and assigned to a user.

The terms of the Infinity software license agreement establish and specify the number of available client accounts in the system configuration. Amtelco currently offers database size choices of:

1,000 accounts	2,000 accounts
3,000 accounts	6,000 accounts
12,000 accounts	25,000 accounts
50,000 accounts	100,000 accounts

Client Account Security

The client account database is stored in the proprietary command set of the Infinity CTI server application. The Infinity CTI server proprietary command set has a limited vocabulary of commands that allows execution of only pre-assigned client account functions.

Access to the client account database is permitted only to individuals designated for access in the Infinity Supervisor application.

The following statements apply to the security of individual client accounts.

- ✘ Each client account has a unique Source, the route by which calls reach the Infinity CTI server. For client accounts whose calls arrive on DID lines or PBX extensions, this is a unique 3-, 4-, or 7-digit telephone number. For client accounts whose calls arrive on loop lines, this is an Infinity CTI server port number.
- ✘ Call handling and messaging tasks are governed by a limited number of Behaviors resident in the proprietary command set of the Infinity CTI server. Specific Behaviors are assigned during the client account set-up process. They include the ability to restrict operator involvement with incoming calls, by routing them to specific locations, directly to voice mail, to an automated auto-answer attendant and to other client accounts.
- ✘ Individual client accounts can be assigned a unique Fetch Passcode. When a client account is assigned a Fetch Passcode, operators cannot access the account information without first entering the proper passcode.
- ✘ Individual client accounts can be designated for Private Voice Mail during the client account set-up process. This feature denies access to voice messages by operators.
- ✘ Each Client Account can be assigned a unique voice mail check-in passcode. This feature denies access to an account's voice messages if the passcode is not entered or is entered incorrectly.

Information Compatibility

The Infinity CTI server allows access to the client account database with an application called the Infinity Client Importer Exporter (ICIE).

The ICIE application is constructed on the Microsoft Windows 95/98/NT platform. This enables the incorporation of all the security and functionalities of the Windows operating system into the application, including, but not limited to, encryption, usage tracking and user access.

The ICIE application requires a Windows 95/98/NT workstation connected to the Infinity CTI server through a TCP/IP network connection.

The ICIE application can function in three modes:

The **Import All mode** is used to bring data from a Microsoft Access database or tab-delimited file into the Infinity client account database by creating new client accounts from the imported data. Infinity client account database fields that are not present in the Access database or tab-delimited file are either left blank or retain their default settings.

The **Import Update mode** is used to revise fields that currently contain information in the Infinity client database for a range of accounts. The importation process does not affect infinity client account database fields that are not present in the Access database or tab delimited file.

The **Export mode** is used to convert the Infinity client database into an Access database or tab-delimited file. The resulting file can be used for searching and editing, or for backup purposes. It also can be used to populate other databases.

HL7 Compatibility

The Infinity CT server supports an interface to existing healthcare information systems to receive real-time patient information using the Hospital Level 7 (HL7) protocol.

The HL7 interface is constructed on the Microsoft Windows 95/98/NT platform. This enables the incorporation of all the security and functionalities of the Windows operating system into the application, including, but not limited to, encryption, usage tracking and user access.

The HL7 interface conforms to the HL7 standard protocol and messaging format in version 2.2. Amtelco has implemented the ADT and MFN portions of the HL7 standard for data exchange with the Infinity CTI server.

The HL7 interface is used to populate listings in the Infinity CTI server directory. Infinity Directory information can then be used by operators to transfer calls to patient rooms, to provide callers with patient information, and to accomplish other tasks that depend on the data contained in the HL7 record.

The HL7 interface with Infinity requires a dedicated Windows 95/98/NT workstation connected to an existing data network through a TCP/IP socket. This workstation also connects to the Infinity CTI server through a TCP/IP network connection.

Web Accessibility

The web-enabled solutions offered by Amtelco combine award-winning software applications, state-of-the-art hardware, proven telecommunications technology and high-speed Internet connectivity to ensure that Internet traffic is always available, effective and secure.

Amtelco provides web-hosting services that can be installed on the premises of healthcare facilities, universities, telephone answering services, executive suites and contact centers. On-site hosting operations require a considerable investment in hardware, software, operations staff and expertise, and the connectivity to the telephone network for transmission capabilities.

Amtelco also offers remotely hosted web services, with all hardware, software operations and staff located off-premise at a separate, but highly secure, facility.

Web Application Configuration

The Infinity web-enabled applications require that a separate web server be connected to the Infinity CTI server through a TCP/IP network connection. The web server must be equipped with the Microsoft Information Server (IIS) Internet accessibility application and its server extensions.

By requiring the IIS application on a separate web server, the Infinity web-enabled applications gain an additional measure of security from the Secure Socket Layer (SSL) feature of the IIS application. The SSL feature utilizes public key encryption to shield network sessions from interception during transmission.

The SSL public key algorithm is comprised of two separate and distinct elements: a private key that is held by the owner of the key pair and a public key that can be distributed to authorized users. The algorithm specifies that one of the keys is used to encrypt transmissions and the other is required to decrypt transmission.

SSL keys are available from a number of vendors; however, Amtelco does not provide SSL keys as an element of its web-enabled applications.

Web Application Security

The Infinity web-enabled software applications are constructed on the Microsoft Windows 95/98/NT platform. This enables the incorporation of all the security and functionalities of the Windows operating system into the applications, including, but not limited to, encryption, usage tracking and user access.

The Infinity web-enabled software applications are maximized for use with the Microsoft Internet Explorer 5.0 web browser software.

The Infinity web-enabled software applications also incorporate the security measures contained in the Infinity Host CTI server application, as well as the Infinity Supervisor and Infinity Telephone Agent workstation applications.

Hosted Web Services

Amtelco offers remotely hosted web services through a partnership with a world-class data center, with operational nodes in Madison, Milwaukee and Appleton, Wisconsin, Grand Rapids, Michigan, and Minneapolis.

Telephone Connectivity

The telephony backbone of Amtelco's remote hosting network is built on one of the most reliable and scalable telecommunications infrastructures available, the OC-48 SONET Ring. Though OC-48 provides a high-traffic capacity (2.488 Gbps), its major benefit is reliability.

The data center contracts with Ameritech and AT&T to maintain a SONET fiber-ring connection between two local central offices and two data center nodes. Should a break occur anywhere in the SONET ring, traffic is rerouted automatically and the ring operates in backup mode, with no loss in capacity, until the break can be repaired.

Internet Connectivity

Call volumes are balanced between four 45-Mbps DS-3 connections to four Internet service providers – AT&T, MCI, GTE and NorLight – to guarantee Internet access for 100 percent of the traffic on the remote hosting network. Trace-route functions, specifically designed to identify response time delays in the Internet connections, are performed on an automated, continual basis. Should one Internet connection fail or experience an unacceptable response time, the remaining connections possess the capacity to handle the full workload.

System Reliability

The remote hosting network operated by Amtelco and the data center provides continual service to all customers. A multiple firewall structure provides secure access to the router. Clustered web servers and high-speed network connectivity to clustered database servers provide fast and accurate transaction processing. Both the servers and the network are monitored 24 hour, 7 day a week to ensure maximum performance.

All core equipment is fully redundant, including the use of redundant power supplies in each unit, to ensure system reliability. Every critical device, including routers, switches and servers, is covered by full-service maintenance contracts that include guaranteed parts replacement within four hours.

All key system thresholds – including bandwidth, CPU, memory and hard disk utilization – are monitored continually to ensure that proper performance levels are maintained. Web site performance and all server operations also are monitored regularly. If any threshold is exceeded, or any failure occurs, Amtelco and data center technicians are alerted to the problem immediately and automatically.

Maximized Server Uptime – Due to the mission-critical design of the hosting network, any server can be taken off line for maintenance or upgrade with no loss of service. When a server is being upgraded, a redundant server handles the workload without interrupting productivity. Back-ups are performed on a regular basis on all servers to guard against any appreciable loss of data.

Telephony Server Integration – Amtelco’s award-winning Infinity telephony server provides full-featured call distribution and messaging functionality as well as connectivity to the hosting network through Amtelco’s several web-enabled software applications.

Web Server Capability – Amtelco’s Windows 2000 web servers also run Microsoft’s Internet Information Server software. The web server configuration can accommodate several thousand hits per second and is configured for ease of expansion as traffic volumes increase.

Database Server Dependability – Amtelco’s Windows 2000 database servers also run Microsoft’s SQL Server database application. Each database server includes a RAID 5 SCSI Disk Array to provide fault tolerance and fast access to data.

Standardized Network Equipment – The data center uses only Cisco equipment in its network. This standardization provides a single point of contact for all issues and enables development of extensive staff skills with the network operating system, Cisco’s Internet Operating System (IOS).

System Security

The data center is environmentally controlled and features state-of-the-art physical and electronic security measures, including multiple network firewalls and digital video site surveillance. The data center features 24 hour, 7 day a week monitoring of the system and its network links by a team of trained and experienced professionals working in the on-site Network Operations Center.

Network Monitoring – A suite of network monitoring tools continually scrutinizes all aspects of the hosting network, from telecommunication circuits to web servers. The possibility of a system failure is all but eliminated by redundancy in all core network components. Should a failure occur anywhere in the hosting network, the technical support staff is immediately notified of the component that has failed and can take appropriate corrective action.

Power Failure Protection – The data center is serviced by dual, independent, electrical circuits and is equipped with two levels of on-site power protection. Uninterruptible Power Supplies (UPSs) immediately deliver electricity to the core equipment should power be lost. An on-site diesel generator protects against long-term electrical service outages that the UPSs are not designed to relieve.

Complete Environmental Controls – The data center is equipped with a number of controls to ensure that environmental conditions are closely monitored and maintained. These measures include temperature, humidity and smoke/fire detection. All environmental information is integrated with the hosting network monitoring system and automated alerts are generated when conditions exceed predetermined thresholds.

Total Security Construction – The data center is constructed entirely of steel and steel-reinforced concrete. It is entirely free of glass windows and unsecured entry points. Biometric hand scanning technology provides strict control of site access. Digital security cameras throughout the data center enable the Network Operations Center to continually monitor activity inside and outside the facility.

1 CALL

a division of

amtelco

4800 Curtin Drive, McFarland, Wisconsin USA 53558-9424

American Tel-A-Systems Inc.