Security Checklist

HiPath 3000 V9

Version: 1.2
Date: 2012-05-21

SEN VA SME PSM / OpenScale Baseline Security Office
Siemens Enterprise Communications

A31003-H3590-P100-1-76A9

Siemens Enterprise Communications
www.siemens-enterprise.com

SIEMENS

Table of Content

1 Introduction

1.1 General Remarks

Information and communication - and their seamless integration in "Unified Communications and Collaboration" (UCC) - are important and valuable assets for an enterprise and are the core parts of their business processes. Therefore, they have to be adequately protected. Every enterprise may require a specific level of protection, which depends on individual requirements to availability, confidentiality, integrity and compliance of the used IT and communication systems.

Siemens Enterprise Communications attempts to provide a common standard of features and settings of security parameters within the delivered products. Beyond this, we generally recommend

- to adapt these default settings to the needs of the individual customer and the specific characteristic of the solution to be deployed
- to outweigh the costs (of implementing security measures) against the risks (of omitting a security measure) and to "harden" the systems appropriately.

As a basis for that, the Security Checklists are published. They support the customer and the service in both direct and indirect channel, as well as self-maintainers, to agree on the settings and to document the decisions that are taken.
The Security Checklists can be used for two purposes:

1. **In the planning and design phase** of a particular customer project:
   Use the Security Checklists of every relevant product to evaluate, if all products that make part of the solution can be aligned with the customer's security requirements – and document in the Checklist, how they can be aligned.
   This ensures that security measures are appropriately considered and included in the Statement of Work to build the basis for the agreement between SEN and the customer: who will be responsible for the individual security measures:
   - During installation/setup of the solution
   - During operation
2. **During installation and during major enhancements or software upgrade activities:**
   The Security Checklists (ideally documented as described in step 1.) are used to apply and/or control the security settings of every individual product.

Update and Feedback

By their nature, security-relevant topics are prone to continuous changes and updates. New findings, corrections and enhancements of this checklist are being included as soon as possible.
Therefore, we recommend using always the latest version of the Security Checklists of the products that are part of your solution.
They can be retrieved from the partner portal Siemens Enterprise Business Area (SEBA) at the relevant product information site.

We encourage you to provide feedback in any cases of unclarity, or problems with the application of this checklist.
Please contact the OpenScale Baseline Security Office (obso@siemens-enterprise.com).

1.2 History of Change

Date	Version	What
2011-11-04	1.0	First Release
2012-05-21	1.2	Extended for further optional components
2012-05-21	1.2	Additions for EVM (2.3.8), Port forwarding (3.2.3), OpenStage Gate View (6.5)

1.3 Customer Deployment - Overview

This Security Checklist covers the product **HiPath 3000 V9** with its related optional applications **OpenScape Office** and **HiPath Xpressions Compact** and lists their security relevant topics and settings in a comprehensive form for the specific customer installation.

	Customer	**Supplier**
Company Name Address Telephone E-Mail		
Covered Systems (e.g. System, SW version, devices, MAC/IP-addresses)		
General Remarks		
Open Issues to be solved until		
Date		

2 HiPath 3000 V9 Hardening Measures in General

This checklist covers the following models and the related integrated or external applications:

HiPath 3300/3350

- 96 Phones
- 24 TDM Phones

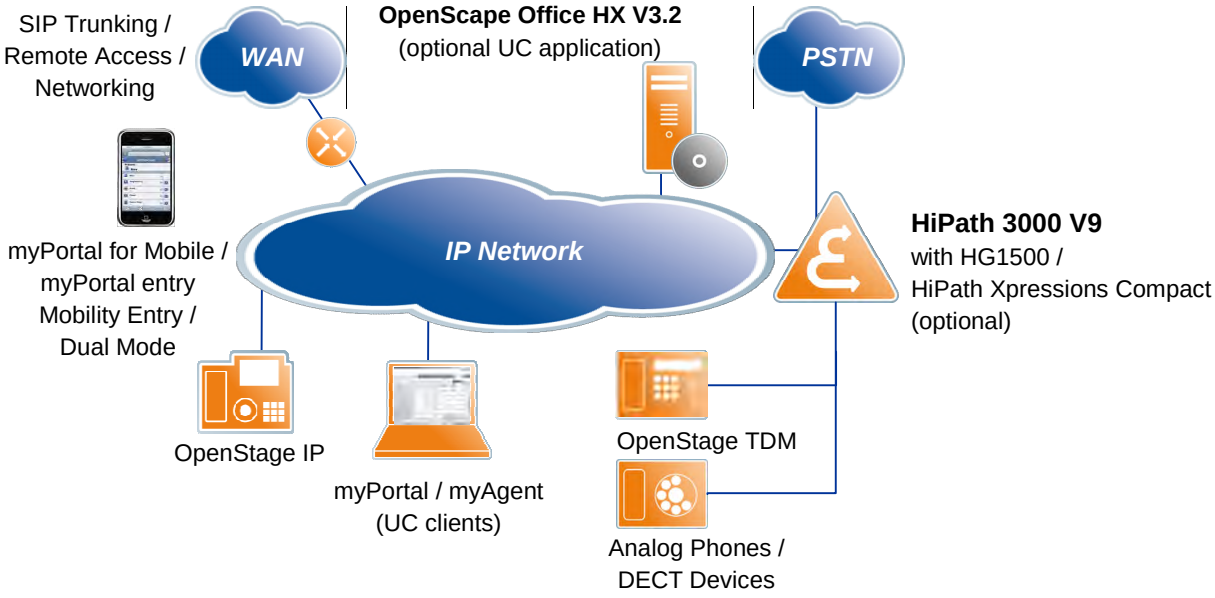
HiPath 3500/3550

- 96 Phones
- 72 TDM Phones

HiPath 3800

- 500 Phones
- 384 TDM Phones

Configuration overview



For safeguarding a HiPath 3000 V9 based communications solution all components have to be considered:

HiPath 3000 is a dedicated appliance providing basic voice services for TDM devices and trunks. Administration access and features like class of service have to be configured carefully. Physical and logical protection of system and infrastructure against manipulation of features as well as sabotage is necessary.

HiPath 5000 RSM (not drawn above) may be used for centralized management of up to 32 networked HiPath 3000 systems. Server and administration have to be secured accordingly. Networking for voice and UC is also possible with OpenScape Office MX/LX - see separate product security checklist [9]

HG1500 is the integrated IP and VoIP gateway, which enables LAN access and routing, IP subscribers, SIP trunking, IP networking and VPN remote access amongst others. It has its own administration via web-based management. Care has to be taken to secure administration and IP interfaces as well as the connected infrastructure.

OpenScape Office HX is the Unified Communications application for HiPath 3000. It uses a dedicated Linux server and has its own web-based management. Protection from unauthorized access and breach of confidentiality has to be enforced through individual passwords and protection of interfaces.

HiPath Xpressions Compact is an integrated voicemail, mobility and conferencing server with its own administration. Special care has to be taken to protect the customer from toll fraud through call forwarding within mailboxes.

Workplace and Server PCs are used for communication clients and central components. Admission control has to be implemented by suitable password, provisioning with actual security updates and virus protection for all involved PCs.

Subscriber Devices (e.g. OpenStage phones, Software Clients) provide the user interface to the phone including unified communications services. On the user and terminal side, security considerations have to be made for desktop and mobile phones as well as for soft clients and the devices they are running on. Access protection in case of absence as well as restriction of reachable call numbers for protection against misuse and resulting toll fraud has to be considered.

Precondition

We recommend strongly always using the latest released software in all components.

CL-1 All components	**Up-to-date SW**		
Measures	Up-to-date SW installed for		
Central Components			
HiPath 3000	Yes: ☐	No: ☐	
HG 1500	Yes: ☐	No: ☐	Not installed: ☐
OpenScape Office HX	Yes: ☐	No: ☐	Not installed: ☐
HiPath Xpressions Compact	Yes: ☐	No: ☐	Not installed: ☐
PCs / Servers			
Server for OpenScape Office HX	Yes: ☐	No: ☐	Not installed: ☐
Server for TAPI	Yes: ☐	No: ☐	Not installed: ☐

Server for HiPath 5000 RSM	Yes: ☐	No: ☐	Not installed: ☐
Other	Yes: ☐	No: ☐	Not installed: ☐
Devices			
OpenStage phones	Yes: ☐	No: ☐	
Other	Yes: ☐	No: ☐	Not installed: ☐
Clients			
OpenScape Office (myPortal, myAttendant, myAgent, ...)	Yes: ☐	No: ☐	Not installed: ☐
OpenScape Personal Edition	Yes: ☐	No: ☐	Not installed: ☐
other	Yes: ☐	No: ☐	Not installed: ☐
Comments, Reasons, References			

The following chapters list the recommended measures for the HiPath 3000 V9 solution.

2.1 System Access Protection

The administration of the system and the involved components has to be protected from unauthorized access. This includes the following aspects:

- Authentication of every user (user name, password, digital certificates)
- Authorization (roles and privileges)
- Audit (activity log)

Fixed or easy to guess passwords are a serious security risk. In any case, individual and complex passwords must be used for all users. Every user shall only get those rights or roles, which are necessary for him.

CL-2 Organizational	Overall password and role concept
Measures	• Name responsible persons with their roles • Define rules for password handling
Customer Name(s) / Role	Yes: ☐ No: ☐
Service Name(s) / Role Name(s) / Role	Yes: ☐ No: ☐
Comments, Reasons, References	

Access to central components like HiPath 3000, OpenScape Office HX server or LAN switches and routers shall only be possible for technicians and administrators.
Personal data, communication data and communication content like voicemails are stored in the communication solution. Confidentiality has to be assured through protection of the administration. The backup data at external drives or servers has to be safeguarded as well.

CL-3 Organizational	Access control to infrastructure and data storage
Measures	• Lock physical access to systems and storage devices and define access rules • Protect files with passwords, where possible
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

2.2 Administration

Secure communication for local and remote administration access is especially important.

2.2.1 HiPath 3000 - Manager C/E

Use only variable password concept. The fixed password concept must not be used.
Password has to be numerical if administration via telephone is needed see 2.2.2

CL-4 HiPath 3000 / Manager E	**Change initial passwords**
Measures	• Select a strong password for all user groups according to chapter 9.1 o Customer o Service o Development
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

2.2.2 HiPath 3000 – Assistant T/TC

Administration by phone is possible from the first two system phones (UP0E). The same passwords as for Manager E are applicable.

CL-5 Assistant T/TC	**Protect administration access by phone**
Measures	• Assign the first two system phones to administrators or trusted users. Do not deploy those phones in places with visitor access.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

2.2.3 HG 1500 Web-based Management

The password is the same as for Manager E (customer, service and developer)

CL-6 HG 1500	**Use HTTPS**
Measures	Use HTTPS that is already default. Avoid reverting to insecure mode (WBM Explorers->Security->SSL).
Executed	Yes: ☐ No: ☐

Comments, Reasons, References	

2.2.4 HiPath 5000 Real Time Services Manager

Secure the PC on which HiPath 5000 RSM is installed. Latest security updates from Operating System vendor should be applied according to checklist items in Section 7 and checklist item CL-1.
There is no separate administration interface; the RSM is running as a Windows service (DBFS).

2.2.5 Administration Access from Applications

The AMHOST (Administration and Maintenance via HOST) feature allows applications (Plus products) to read certain system information and to change it, if necessary. To enable applications to access the system, you have to set up a user without a user group in the HiPath 3000 default user administration. It is enabled by default and has "77777" as password. It should be changed from the default with a strong password.
You can only change this password if the system is configured using a variable password. In this case, delete the "AMHOST" user and re-configure the system with the same user name and a new password. Please note that the same password has to be configured in the application (Plus Product).

CL-7 HiPath 3000	**Configure AMHOST password**
Measures	The measures that can be performed based on customer needs are: • Disable AMHOST user if this interface is not used. • Select strong password conformant with section 9.1 for the AMHOST user.
Executed	Yes: ☐ No: ☐ Disabled ☐
Comments, Reasons, References	

2.2.6 Remote Administration HiPath 3000 / 5000

There are several possibilities for remote administration and maintenance with different security levels.

SIRA / SSDP
This is the recommended secure connection to the SEN service center. Call back and a strong password has to be used (see 9.1).
The Smart Services Delivery Platform (SSDP) provides a secure broadband connection, which is initiated from the customer network. It is realized using an external "plug PC "(option). For securing this device see 6.7 .

VPN
Secure tunnel shall be use for remote administration via IP. This can be implemented via HG 1500 or an external VPN router (see also 3.3.)
Direct access from internet must not be used, as this brings high risks from Internet attacks.

Remote Access over ISDN / BRI
Remote Access over ISDN / BRI (incoming connection) should be used only with call back.
It is also possible to request access rights from the customer for every single remote service activity.

CL-8 HiPath 3000	**Secure Remote Administration Access**
Executed	Yes: ☐ No: ☐ No remote access: ☐
Comments, Reasons, References	Used variant (SIRA, SSDP, VPN, ISDN)

2.2.7 0nline User

Online user allows to simulate a phone and can set up calls or features for service purpose. Online user connects to the system with Manager E credentials. It is enabled by default. The Telnet protocol in use can be blocked by Firewall rules, if necessary..

CL-9 HiPath 3000	**Disable Telnet (option)**
Measures	• If this service is not wanted, the access can be blocked. (Manger E : Settings, Network, Firewall, activate IP firewall port 23 and/or application firewall)
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

2.3 Communication Access and Toll Fraud Protection

Toll fraud can lead to considerable phone charges. The following measures have to be observed to protect against unauthorized calls through HiPath 3000.

2.3.1 Class of Service

HiPath 3000 provides calls to external destinations either directly from the phone or through call forwarding and 3rd party call control. This includes foreign and special call numbers with high charges. The reachable call destinations shall be restricted to the necessary numbers for toll fraud protection. This has to be considered also for Modem and Fax ports.

CL-10 HiPath 3000	Toll restriction for devices
Measures	Suitable Class of Service (COS) is assigned for every device [1] chapter 9.7: • Internal or outward-restricted trunk access for devices, where no external calls are needed (emergency calls still possible). • Allowed Lists configured for necessary business connections, other destinations are blocked. • Denied Lists configured to block special numbers or countries (as an alternative least cost routing (LCR) may be used). Further possibilities: • Setup COS for trunk group connections (which trunk group is allowed to connect with which trunk group) in “Group assignment” and then “CON Matrix) • Delete the “call forwarding external” flag for all devices, which do not need it, especially for devices within reach of external persons. • Disable the three “Transit permission” flags in system parameters if no transit traffic is needed (reduces danger of toll fraud).
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

Notes:
- The class of service may also be restricted depending on time and date with COS changeover or night service.
- All conducted calls are logged in the system and can be checked with an accounting tool. For logging incoming calls, the flag “Log incoming calls” in Call Charges > Output format must be activated. Internal node calls and transit calls are not logged.
- Alarms can be configured for an attendant console in case of trunk resources occupied from external – external connections. It is possible to release such calls (toll fraud feature).

2.3.2 Associated Dialling and Services

Associated Dialling / Services allow e.g. call setup or activation of call forwarding for other stations. Assign rights only to subscribers who need them to avoid misuse.

CL-11 HiPath 3000	Restrict Associated Features
Measures	• Enable the station flag only for users who need the function. • Inform concerned users about handling and security risks. See [1] section 4.2.1
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

2.3.3 Direct Inward System Access (DISA)

The DISA feature allows call setup to external destinations and feature programming from external e.g. for call forwarding. Unrestricted access to DISA could be used by unauthorized parties for toll fraud. Access to DISA should be restricted.

CL-12 HiPath 3000	**Restrict DISA access**
Measures	• If DISA is not used, no DISA number must be configured. • The feature is enabled only for users who need the function. • Inform DISA users about handling and security risks. See[1] section 6.5
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

The feature DISA has to be protected by an individual password (PIN) if it is enabled.

CL-13 HiPath 3000	**Change default PIN for DISA**
Measures	• The PIN used for DISA is the same as for individual code lock. It has to be set to an individual value by every DISA user. A 5-digit sequence, which cannot be guessed easily, has to be selected (see 9.1). • Information and briefing of the DISA users.
Executed	Yes: ☐ No: ☐ DISA not used ☐
Comments, Reasons, References	

2.3.4 Mobility Entry

The feature Mobility Entry allows phone calls via HiPath 3000 and feature activation for authorized users. The subscriber is identified through his transmitted phone number. The devices, which are registered for this service, shall be protected from unauthorized access. A small risk for toll fraud lies in pretending a registered calling number by fraudulent callers (CLIP no screening, possible via some VoIP providers).

CL-14 Mobility Entry Devices	**Protect the devices registered for DISA / use call back**
Measures	• Protect registered devices from unauthorized access (e.g. PIN for mobile phones). • Use call back for enhanced security. • Information Mobility Entry users.
Executed	Yes: ☐ No: ☐ Mobility not used: ☐
Comments, Reasons, References	Callback Yes ☐ No ☐

2.3.5 Mobile Users

IP mobility is activated by the system wide flag 'relocate allowed'. It is recommended to activate authentication in this case.

CL-15 Mobility Entry Devices	**Protect the access of mobile users**
Measures	• For mobile users 'Authentication at the communication system' is activated at Manager E • A strong password has to be set up.
Executed	Yes: ☐ No: ☐ Mobility not used: ☐
Comments, Reasons, References	

2.3.6 Access to Phones

For places with visitor access or with special functions, it is recommended to protect the phone access by code lock. Special functions are for instance system phone lock (COS changeover), switch night mode, associated dialling and silent monitoring / call supervision as well as phone lock reset for other phones. Code lock is handled via phone menu or key.

FlexCall (call from any device with own authorization) is protected by the code lock PIN as well.
For mobile users (logon at any device) the authentication password for the mobile user has to be activated.

CL-16 System phones	**Code lock activated**
Measures	• For devices with danger of misuse, code lock is used with an individual 5-digit PIN which is not easy to guess (see 9.1). • Information and briefing of phone users
Executed	Yes: ☐ No: ☐

Comments, Reasons, References	

2.3.7 Door Opener

HiPath 3000 provides activation of door openers via phone.

CL-17 HiPath 3000	**Restrict authorization for door opener**
Measures	• Authorization is assigned only to those stations, where necessary. • Remote access to door opener is not possible.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

2.3.8 Entry Voicemail (EVM)

Change the initial PIN to an individual safe value to secure mailboxes against unauthorized access and forwarding of external calls via mailbox.

CL-18 Entry Voice Mail	**Activate individual PIN**
Measures	• Users are instructed to use individual strong PINs for all personal and attendant mailboxes • Set Class of Service (COS) for the EVM ports (see 2.3.1) to 'outward-restricted' for day and night service
Executed	Yes: ☐ No: ☐ Not used: ☐
Comments, Reasons, References	

Note: If call forwarding out of mailboxes is needed, e.g. for auto attendant, COS shall be extended carefully only to those destinations, which are allowed to be reached.

2.4 Confidentiality of Communications

2.4.1 Transmission via internal IP networks (LAN)

For the internal IP network, the requirements according to the administrator documentation have to be met. Access to central components like switches and routers shall be restricted to technicians and administrators.
A logical or physical decoupling of voice and data network should be considered depending on the existing infrastructure. The IT service provider of the customer may have to be involved.

CL-19 **LAN infrastructure**	**Protect infrastructure**
Measures	• Access to routers and switches only for authorized persons and trusted devices • Use separate VLAN for voice communication (optional)
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

2.4.2 Signalling and Payload Encryption

For confidentiality and integrity of VoIP communication, the activation of signalling and payload encryption (SPE) shall be considered. Connections where the OpenScape Office application is involved in the payload can currently not be secured. SIP clients registered to HiPath 3000 do not support SPE.

CL-20 HiPath 3000 / HG 1500	**Signalling and Payload Encryption**
Measures	• SPE support system wide flag activated (Manager E) • Payload Security activated for all relevant subscribers (Station view) • Certificates imported to HG1500/STMI (.CRT-root, .PKCS12-peer) • TLS has been selected for transport on the IP end-points (HFA WBM or device configuration interface) • For secure IP-trunk parameter "Security Level of Node Encryption:" in the Voice Gateway menu has to be set to "Secure" (WBM). This is not available for ITSP connections. • Make Setting, if gateway calls are considered as secure (influences display at devices). • Enable certificate Handling alarms (In HG1500 WBM, Check that an e-mail is sent to the administrator when events involving SPE certificates occur (Maintenance → Events → Reaction Table → MSG_SPE_CERT_*)
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

2.4.3 Call Supervision

For certain countries the feature Call Supervision (Silent Monitoring) is available. Please observe the legal regulations in your countries.
It shall be assured by protection of administration access (see chapter 4) and of authorized devices (see chapter 2.2.4) that this function is not misused.

CL-21 HiPath 3000	**Restrict Call Supervision (Silent Monitoring)**
Measures	Subscriber authorization and possible targets are restricted to the minimum needed.
Executed	Yes: ☐ No: ☐ Not used/available: ☐
Comments, Reasons, References	

2.4.4 IP Transmission with Public Networks

VoIP access to public networks is based usually on a user account and password delivered by the provider. This data is entered at the HiPath 3000 / HG1500 administration and has to be kept confidential. For extended security, a provider with a dedicated line or secure VPN access is recommended.

CL-22 Infrastructure	Access to VoIP Network
Measures	• Secure VoIP trunk access is used (VPN, dedicate line). • Account data is kept confidential
Executed	Yes: ☐ No: ☐ Not used/available: ☐
Comments, Reasons, References	Basic ☐ VPN ☐ dedicated line ☐

2.4.5 External Subscribers

External subscribers like tele-workers or mobile workers shall be connected via VPN to protect confidentiality and to avoid misuse of the subscriber access by unauthorized persons. With VPN, an encrypted tunnel is set up for the communication. This can be done by HiPath 3000 / HG 1500 or by an existing VPN Router.
For VPN details see chapter 3.3

CL-23 Infrastructure	Access for external subscribers only via VPN
Executed	Yes: ☐ No: ☐ No ext. subscriber: ☐
Comments, Reasons, References	

2.4.6 Networking for HiPath 3000

Protection of the IP connections for networking between different sites by VPN is strongly recommended to protect confidentiality and to avoid misuse by unauthorized persons. This can be done by HiPath 3000 / HG 1500 or by an existing VPN Router. Voice communication, UC communication and administration take place via this IP connection.
For VPN details see chapter 3.3.

CL-24 Infrastructure	IP Networking only via VPN
Executed	Yes: ☐ No: ☐ No networking: ☐
Comments, Reasons, References	

2.5 Availability

HiPath 3000 and OpenScape Office were developed for high reliability. This can be enhanced by measures in the infrastructure.

CL-25 Infrastructure	**Enhanced Availability**
Measures	• A possible weakness is electrical power supply. For countries with higher probability of power outages, a separate uninterruptible power supply (UPS) for OpenScape Office and related components may be sensible. • Two or more independent public network trunks extend availability in case of carrier failures. • For the server-based OpenScape Office HX, a server with redundant power supply and/or hard disk with SW RAID can be used. Higher availability can be achieved by using a suitable virtual server environment (please see current release documentation).
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	Please describe measures taken:

2.6 Emergency Calls

Provisions shall be taken that emergency calls can always be made.

CL-26 HiPath 3000	**Emergency calls available**
Measures	• Enter all relevant emergency call numbers for class of service. • Provide a separate circuit switched telephone line, if VoIP trunks without emergency call support are used. • USA only: Configure the local identification number (LIN) for the E911 service. • Configure LCR to show correct local area code.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

3 IP Interfaces

3.1 LAN Interfaces and Ports

Interfaces, which are not used, are deactivated by default and shall not be activated without explicit need.
The ports used with HiPath 3000 / HG1500 can be found in the appendix C of the administrator documentation [2]. This information may be used for external firewall configuration e.g. for network separation to increase security.

3.1.1 LIM Interface and HG 1500 LAN interfaces

The HiPath 3000 LAN Interface Module (LIM) is used for administration via Manager E/C and other IP services.
The LIM interface is automatically deactivated if HG 1500 is present..

The gateway module HG1500 provides two LAN interfaces with higher performance and additional services.

For both interfaces, the following rules apply.

Limit access to the HiPath 3000 administration port to the administrator's PC. Manager E should only be accessible from the administrator's machine.

CL-27 HiPath 3000	**Restrict access to the Manager E port**
Measures	Access to the Manager-E port (TCP port 7000 by default) should be limited to the administrator's PC (IP address / MAC address). This can be done by the Manager E firewall configuration.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

TFTP is a protocol used to download configuration data and SW update. Access to TFTP ports should be restricted to the administrator's PC and HiPath 5000 RSM servers.

CL-28 HiPath 3000	**Restrict access to TFTP ports**
Measures	• Access to the TFTP port (UDP port 69 by default) should be limited to the administrator's PC and HiPath 5000 RSM PC (IP address / MAC address). This can be done by the Manager E firewall configuration. • Block the TFTP port for the LIM interface.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

3.1.2 SNMP Interface

The Simple Network Management Protocol Interface (SNMP) allows transmission of error messages. It is present in HiPath 3000 and HG 1500.

The SNMP (V1) interface is not activated by default.
If used, a restriction of read and write access is necessary. A detailed description can be found in the administration manuals [1] and [2].

CL-29 HiPath 3000	**SNMP Interfaces secured**
Measures	• Restrict read and write access to defined IP addresses with individual community name. • Disable "Enable SNMP" flag, if SNMP is not required.
Executed	Yes: ☐ No: ☐ Deactivated: ☐
Comments, Reasons, References	

3.1.3 CSTA Interface

The Computer-supported telecommunications applications (CSTA) interface allows monitoring and control of devices, which are connected, to HiPath 3000. This functionality is used by OpenScape Office HX and direct via CSTA interface or via TAPI 120/170 middleware by 3rd party CTI applications. Attackers with LAN access and CSTA knowledge might exploit this to initiate calls. CSTA is active by default.

CL-30 HiPath 3000	**Disable or limit CSTA access**
Measures	• Limit access to specific servers using application firewall (IP addresses and protocols) or IP firewall (IP addresses and MAC addresses) or block access if not needed
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

3.1.4 LDAP Interface

The Lightweight Directory Access Protocol (LDAP) is used for access to external databases. Unauthorized access may disclose company directory data. The interface is disabled by default.

CL-31 LDAP Server	Protect LDAP access
Measures	Set up strong LDAP password at LDAP Server and HiPath 3000.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

3.2 Router / Proxy

The following recommendations apply to the router integrated with HG 1500 as well as to an external router, which is mandatory for SIP trunking with ITSP.

3.2.1 IP Address Filtering

IP Address Filtering protects HG 1500 against unauthorized access for example via an external network or an internal or external PC. If IP address filtering has been activated, access to the released IP addresses is restricted. Use Firewall activation with care since you can lose all access to HG 1500.

CL-32 HG 1500 / external Router	IP address filtering (optional)
Measures	• Enable IP address filtering for configuring the firewall, if it is seen necessary and does not hinder administration access (WBM at Explorers, Security see [2])
Executed	Yes: ☐ No: ☐ none active: ☐
Comments, Reasons, References	Please document IP address filtering

3.2.2 MAC Address Filtering

MAC address filtering protects HG 1500 against unauthorized access (via an external PC, for example). Only PCs with IP addresses that are released in combination with the relevant unique MAC address via this security function are assigned access authorization. If the IP and MAC addresses do not match those of the specified combination, access is denied. This is effective only for the local IP subnet.

CL-33 HG 1500 / external router	MAC address filtering (optional)
Measures	• Enable only selected MAC addresses, if it is seen necessary and does not hinder administration access (WBM at Explorers, Security, see [2])
Executed	Yes: ☐ No: ☐ none active: ☐

Comments, Reasons, References	Please document MAC address filtering.

3.2.3 NAT Port Enabling / Port Forwarding

For some Internet applications, specific ports have to be enabled and forwarded to the internal LAN by Network Address translation (NAT).

- Port forwarding is not active by default.
- Please use this feature with care. The firewall is no longer in place for those ports. The communicating applications shall meet extended security standards e.g. by encryption and efficient access control and robustness against denial-of-service attacks and message floods.
- A web proxy in a DMZ may enhance security, but can lead to limitations with some devices and browsers.

Notes:

- Port Forwarding must not be used for external VoIP subscribers as this bears the risk of toll fraud by unauthorized access. Please use only VPN for remote IP subscribers.
- Port Forwarding must not be used for application access e.g. by OpenScape Office clients or CSTA applications from external. These interfaces are not secured and might be eavesdropped and misused.

CL-34 HG 1500 / external router	**Port Forwarding inactive or restricted**
Measures	• Check necessity and risk. • Delete non-essential port forwardings.
Executed	Yes: ☐ No: ☐ none active: ☐
Comments, Reasons, References	Please document forwarded ports and usage

3.2.4 PPP Configuration

The PPP protocol is sometimes used for Internet and ISDN data access.
PPP shall be used with CHAP authentication if supported by the communication partner.
CHAP is preconfigured in HiPath 3000 within "Routing PSTN". This protocol is used for remote ISDN access to HiPath 3000 and / or HG1500.

CL-35 HiPath 3000 / external router	**PPP configuration with CHAP is active** (no change to default)
Measures	Keep CHAP setting and use strong password
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

3.3 Secure Tunnel (VPN)

Secure tunnels are strongly recommended for networking as well as for remote access. For every VPN remote subscriber a dedicated authentication shall be selected. This allows easy blocking of a remote access e.g. when an employee leaves the company.

Recommended operation mode:
IKE "Main Mode" with Perfect Forward Secrecy and DH Group 2 / 5 (Default)
Encryption with AES (check setting in the VPN Client)

A) Pre-shared Key (Recommended only for a limited number of devices)
Chose key word according to password recommendation (chapter 9.1)
A secure transmission and storage of the key word has to be guaranteed

B) Certificates shall be used for increased security requirements or with an existing PKI Infrastructure.
Recommended operation mode: RSA and hash function with SHA-1
Configuration is more complex (expert mode). Documentation of certificates and serial numbers and safe storage have to be guaranteed.

CL-36 HG 1500 / external router	**Networking and remote access allowed via VPN only**
Executed	Yes: ☐ No: ☐ No networking/remote access: ☐
Comments, Reasons, References	Pre-shared key ☐ Certificates ☐

4 OpenScape Office HX (Option)

Is OpenScape Office HX part of the solution?	Yes: ☐ No: ☐ > continue with chapter 5

For PC and server security requirements see chapter 7

4.1 OpenScape Office Clients

The OpenScape Office application delivers unified communication with personal, attendant and Contact Center clients. Passwords according to the password rules have to be used. For the PC based communication clients an alphanumerical password is possible. In most cases, access to voice mail is also needed from normal phones. To cover that use case, a numerical Password (PIN) has to be used. The minimum recommended and default length is 6 digits.

The following OpenScape Office client applications are available

- myPortal, myPortal for Outlook, myPortal for Mobile, myPortal for OpenStage, Fax driver
- myAgent, myReports
- myAttendant

Client applications allow for instance rule-based call forwarding and automated attendant or conferences. This could be used for toll fraud, if unauthorized persons get access to the applications. To protect from unauthorized access, the general password rules have to be followed for the client software and the devices on which they are running.
Note: Unauthorized access to the call journal and log files at the client PC may disclose the individual communication history of the user.

CL-37 OSO Clients	**Change password for myPortal, myAgent, myAttendant and protect the devices, where they are running**
Measures	• The login password (also used as mailbox PIN, numerical) has to be set to an individual value, by every user (see 9.1) • Unattended PCs and mobile devices must be locked • Information and briefing of all users done
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

4.2 OpenScape Office Administration

4.2.1 Local administration

The access to the OpenScape Office Assistant occurs always encrypted via HTTPS. Administration access is documented in the administration protocol. This protocol shall stay activated.
A self-signed server certificate for HTTPS encryption is delivered by default. This has to be accepted as trusted by the user in the browser.

For server authentication and against man-in-the-middle attacks, an individual certificate is necessary, which relies on a root certificate authority. This enables the browser, used for administration, to set up a secure end-to-end connection with OpenScape Office.

CL-38 **OpenScape Office**	**Customer specific certificate**
Measures	Import a customer certificate, which is issued for the OpenScape Office (server name or IP address) and activate it for the administration access.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

A new password for OpenScape Office Assistant has to be entered after first start according to password recommendations (see chapter 9.1)

CL-39 **OpenScape Office**	**Individual strong passwords**
Measures	Implement user accounts, roles and individual passwords for • Basic user • Advanced user • Expert user
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

4.2.2 Remote Administration OpenScape Office HX

The following options are available:

Smart Services Delivery Platform (SSDP)

SSDP is the most secure access. OpenScape Office sets up an encrypted and authenticated outgoing connection from behind the firewall. This is the **preferred solution**.

VPN Access

A dedicated VPN access is recommended, if SSDP is not available. This is possible via an external VPN router. For VPN see chapter 3.3.

Remote Access over Internet

Remote Access over Internet should be **activated at the most temporarily** for the time of the administration access not to be an easy target for attacks from the Internet. Check 3.2.3 port forwarding for Internet.

CL-40 HiPath 3000	**Secure Remote Administration Access**
Executed	Yes: ☐ No: ☐ No remote access: ☐
Comments, Reasons, References	Used variant:

4.3 IP Interfaces OpenScape Office

4.3.1 SAMBA Share (File Service)

A SAMBA share provides help files to the OpenScape Office clients. It is also needed for first distribution of OpenScape Office client software, and for system backup.
The directories are read-only where possible by default. The service can be switched off, if customer security policy requires that. The functions mentioned above are not available in this case.

CL-41 OpenScape Office	**SAMBA is deactivated (option)**
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

4.3.2 XMPP Interface

The Extensible Messaging and Presence Protocol (XMPP) is used for presence federation and chat (e.g. with Google Talk). The OpenScape Office XMPP server offers encrypted and unencrypted communication. Selection depends on the communication partner. Communicate only with XMPP servers which support encrypted communication, if instant messages and presence status has to be confidential. In this case the default self-signed certificates have to be .accepted.

Note: Port-forwarding for TCP port 5269 has to be activated to be able to use XMPP via WAN (see 3.2.3)

CL-42 OpenScape Office	**Secure XMPP communication**
Measures	Use an external XMPP Server which supports secure communication. Remark: servers who do not accept self-signed certificates can not be used.
Executed	Yes: ☐ No: ☐ XMPP not active: ☐

Comments, Reasons, References	Used external XMPP Server :

4.3.3 Web Services

Web Services are offered by OpenScape Office HX for use by the web-based clients

- myPortal for Mobile
- myPortal for OpenStage
- customer specific applications

It is recommended to use HTTPS for secure communications. For mobile devices with low performance, it may be necessary to use HTTP instead. HTTP has be used also for the OpenStage V2 devices.
The cookie, which is saving the password, shall be disabled, if there is a risk that an unauthorized person gets access to the mobile device. This has the disadvantage for the user, that manual password entry is necessary every time. The user password is the same as for the other OpenScape Office clients.

Note: Port-forwarding for port 8802 (HTTPS) or 8801 (HTTP) has to be activated to be able to use the Web Services via WAN (see 3.2.3). To increase security for the internal LAN, an external web proxy can be used.

CL-43 **OpenScape Office HX**	**Secure Access to Web Services**
Measures	• Only 'HTTPS' is activated in OpenScape Office Assistant • 'Save login data to device' is disabled
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	Describe measures taken:

4.3.4 SMTP Interface

Simple Mail Transfer Protocol (SMTP) is used to send mails to users and administrators and to receive mails for Contact Center agents. Encryption is recommended. SMTP can only be used with encryption when the used mail server supports that.

CL-44 **OpenScape Office**	**SMTP Interface secured**
Measures	• Select secure communication at WBM > Service Center > Email Forwarding • Select 'Use SSL' for inbound e-mail services at Application Suite > OpenScape Office > Contact Center

Executed	Yes: ☐ No: ☐ Deactivated: ☐
Comments, Reasons, References	

4.3.5 LDAP Interface

The Lightweight Directory Access Protocol (LDAP) is used in OpenScape Office for access to external databases as well as for providing subscriber information to other applications and clients. Unauthorized access may disclose company directory data. The interface is disabled by default.
Port 389 has to be opened for access to the integrated LDAP server within Linux.
Please make sure to use strong passwords also for external LDAP servers.

CL-45 OpenScape Office	**Protect LDAP access**
Measures	Set up strong LDAP password at OpenScape Office Assistant for the integrated LDAP server (expert mode, application suite) see 9.1
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

5 HiPath Xpressions Compact (Option)

Is HiPath Xpressions Compact part of the solution?	Yes: ☐ No: ☐ > continue with chapter 6

Inadequate handling of mailbox passwords by customers increases the risk of toll fraud. This can happen via the use of substitute or auto attendant features. In order to avoid such issues, the measures described below must be taken.

5.1 Administration

Outgoing traffic should be blocked from HiPath Xpressions Compact for day and night service, by setting all IVM ports to system class of service (COS) 'outward restricted' from HiPath 3000 Manager E.
In recent versions of HiPath 3000 Manager E this is the default. it is therefore advisable to use an up-to-date version of Manager-E and not change the default setting.

CL-46 HiPath Xpressions Compact	**Limit IVM Ports Class of Service to 'Outward-restricted'**
Measures	• In HiPath 3000 Manager E under 'Classes of Service → station' check that the default COS group is 'Outward restricted'. • In Day and Night service the class of service is also set to 'Outward restricted'.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

Also the default Class of Service for IVM mailboxes should be set to COS3 instead of the default COS, if the feature call forwarding to substitute is not needed.

CL-47 HiPath Xpressions Compact	**Limit IVM mailbox Class of Service to COS3**
Measures	• In HiPath 3000 Manager E under 'Auxiliary equipment →Integrated voicemail (IVM)' change the setting from COS4 to COS3 for configured IVM ports.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

By using the IVM WBM, it is possible for the Administrator to view and modify all user accounts by logging in as Superuser. The Superuser PIN should be set according to the recommendations in section 9.1. The maximum length of the Superuser PIN is 8 (configurable from Manager E or Xpressions Compact WBM).
For the administration role 'service' the same credentials as for HiPath 3000 are used.

CL-48 HiPath Xpressions Compact	**Implement a strong PIN for Superuser**
Measures	Choose a strong PIN as described in section 9.1 for the Superuser account in the HiPath Xpressions Compact WBM. This is configured via the 'Mailbox Administration → SU Superuser → General Settings' menu options.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

The DLI login page is also accessible from the HiPath Xpressions Compact WBM, and this introduces the security risk of an unauthorized party altering phone configurations or accessing other privileged information. To avoid the risk it is necessary to change the default password of the DLI user from "DLI" to a more secure combination according to the recommendations in section 9.1.

CL-49 HiPath Xpressions Compact	**Implement a strong PIN for the DLI user**
Measures	Choose a strong PIN as described in section 9.1 for the DLI account. This setting is accessible from within the HiPath Xpressions Compact WBM. This is configured via the 'Basic Settings → Change Password' menu options.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

5.2 Mailbox Protection

Along with these features, it is important to explain the importance of safe mailbox code numbers to the customer, and that they should be kept confidential, non-trivial, and that they protect voice messages and features out of the mailbox. It is recommended to keep the default code number to at least 6 digits. This is the default for updated versions of Manager-E. All users have to change their mailbox PIN immediately. This is enforced during the first mailbox access,. The mailbox PIN is also used for the WBM 'user role'.

CL-50 HiPath Xpressions Compact	**Protect all mailboxes by individual PINs**
Measures	• Each user is instructed to choose a strong PIN as described in section 9.1 • All group mailboxes and autoattendant mailboxes get a strong PIN Note: The setting is accessible from within the HiPath Xpressions Compact WBM.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

Maximum login attempts should be set to 3 to block brute force attacks. (Default for recent versions.)

CL-51 HiPath Xpressions Compact	**Set maximum login attempts to 3**
Measures	In Manager-E, under Auxiliary equipment →Integrated Voice Mail (IVM) → IVM → Additional Settings → Additional
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

The measures described above block toll fraud but they also limit access to the following features:

- Call back external party from voice mailbox
- Message notification call to external destination
- Call forwarding to substitute number
- Auto-attendant for external destinations
- Xpressions Mobility
- Xpressions Conference

If those features are needed, the HiPath 3000 COS for the IVM ports has to be extended with care e.g. to allow only local or national calls.

5.3 IP Interfaces HiPath Xpressions Compact

The LAN interface of HiPath Xpressions Compact is used for

- Voice-mail to E-Mail
- Web-based Management (customer, superuser and service)
- Service tasks like fast SW-update

Several IP ports and services are used for HiPath Xpressions Compact, which cannot be administrated. Please make sure, that access to the LAN interface of Xpressions Compact is not possible from unauthorized devices and especially from the Internet.

Use the application firewall in Manager E to protect specific IVM interfaces.

CL-52 HiPath 3000	**Set up application firewall**
Measures	Restrict access to specific IP addresses for IVM-FTP, IVM-TFTP, IVM-SSH, IVM-HTTP
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

6 Further Components

All released applications and components are documented in the HiPath 3000 V9 sales information or current release note. Please take into account the product-specific security checklists for components, which are included in the solution but not mentioned here.

6.1 HiPath Cordless Office / HiPath Cordless IP (DECT)

For unsecured and inappropriate configurations, eavesdropping attacks at DECT devices have been reported. The following has to be observed to impede such attacks:

Encryption is active for HiPath Cordless DECT devices by default. This setting may be changed only temporarily e.g. for diagnostics.
Only the officially released components out of the Gigaset Professional family shall be used. DECT-Headsets, DECT TAE plugs or other DECT devices can jeopardize confidentiality.

6.2 Wireless LAN (WLAN)

For HiPath 3000 V9 the following WLAN components are released:

- HiPath Wireless AP 2630 / 2640
- optiPoint WL2 professional

Please make sure that a secure transmission like WPA2 is chosen (compare product related security checklist and / or administration manuals).

6.3 TAPI 120 / TAPI 170 / CallBridge IP

These applications provide CTI interfaces for phone call control and monitoring. They run on Windows client PCs or servers and are protected by Windows' own security mechanisms e.g. access control and user accounts. The TAPI middleware makes use of the CSTA interface, see 3.1.3.

Access to the hosting PCs has to be protected. For Server security requirements see chapter 7.

6.4 optiClient Attendant

optiClient attendant is a Windows application which allows call monitoring and call transfer as well as feature control (e.g. call forwarding) for a single system or a network of HiPath 3000 systems. It is connected via USB or LAN at a suitable HiPath 3000 phone.

For the hosting PCs the rules from chapter 7 apply.

Notes:

- SW update is possible via Internet from a fixed IP address.
- The installed number of licenses determines the maximal numbers of simultaneously operational optiClient Attendant applications.
- Network-wide subscriber busy state information is exchanged via IP with a central BLF Server (TCP, default port 3001)

6.5 OpenStage Gate View

OpenStage Gate View is a video surveillance application, which displays camera pictures at OpenStage phones. It is based on a so-called "plug PC", a tiny Linux appliance that can be plugged into the power outlet.
It provides administrator and user access via web-browser. Access has to be restricted to authorized persons.

For picture display at mobile phones, the port 443 has to be accessible from the Internet. For risks see 3.2.3.

CL-53 Gate View	**Secure Passwords**
Measures	• Change the Gate View administration password according to 9.1 • Change the passwords for web access to the used cameras according to 9.1 • Set up user passwords according to 9.1
Executed	Yes: ☐ No: ☐ Not Part of Solution: ☐
Comments, Reasons, References	

6.6 myPortal entry Web Services

myPortal entry Web Services is an entry UC solution for HiPath 3300/3500 which can be used by the web-based clients

- myPortal web
- myPortal entry

An external "Plug PC" is used for this application. If OpenScape Office HX is part of the solution, the web services are provided by OpenScape Office HX (see 4.3.3).

It is recommended to use HTTPS for secure communications. For mobile devices with low performance, it may be necessary to use HTTP instead. HTTP has been used also for the OpenStage V2 devices.
The cookie, which is saving the password, shall be disabled, if there is a risk that an unauthorized person gets access to the mobile device. This has the disadvantage for the user, that manual password entry is necessary every time. Logon of a mobile user with the default password is rejected.

Note: Port-forwarding for port 8802 (HTTPS) or 8801 (HTTP) has to be activated to be able to use the Web Services via WAN (see 3.2.3). To increase security for the internal LAN, an external web proxy can be used.

CL-54 HiPath 3000 Web Services Plug PC	**Secure Access to Web Services**
Measures	• Select a strong Admin password according to 9.1 • Activate only HTTPS • Enable 'Force user to choose secure password' • Disable 'Save login data to device'
Executed	Yes: ☐ No: ☐ Not Part of Solution: ☐
Comments, Reasons, References	Describe measures taken:

6.7 SSDP for HiPath 3000

Smart Services Delivery Platform (SSDP) is available for HiPath 3000 by an optional plug-PC. It provides a secure remote service access.

The component has the ability to store traces on a USB memory stick, if the feature is enabled. The trace data may reveal communication details to persons with technical knowledge. Access to the Plug-PC shall be restricted if required.

Remark: OpenScape Office HX has its own SSDP component.

CL-55 Plug PC	**Secure Password**
Measures	• Secure the administration access is by a password according to 9.1
Executed	Yes: ☐ No: ☐ Not Part of Solution: ☐
Comments, Reasons, References	

7 Desktop and Server PCs

General requirements for all PCs, which run communication clients and applications:

The operating system version is released for the communication software (see sales information)
Current security updates are installed (see [5]).
A suitable virus protection SW shall be installed and active (see [6]). This is especially true for mail servers and Windows PCs.
Access is protected by passwords according to the password rules (see 9.1)

CL-56 Desktop and Server PCs	**Security updates, virus protection and access control are implemented**
Executed	Desktop PCs Yes: ☐ No: ☐ Not part of solution ☐ OpenScape Office HX Server Yes: ☐ No: ☐ Not part of solution ☐ TAPI Server Yes: ☐ No: ☐ Not part of solution ☐ HiPath 5000 RSM Server Yes: ☐ No: ☐ Not part of solution ☐ optiClient Attendant Yes: ☐ No: ☐ Not part of solution ☐ ..... Yes: ☐ No: ☐ Not part of solution ☐
Comments, Reasons, References	PC Operating System / Update Antivirus

The Server PC for OpenScape Office HX shall be kept protected as much as possible. For protection of physical access, see chapter 9
For the Linux-based OpenScape Office HX in a protected environment, threat is considered to be low. There is a risk of degradation of real-time performance by Anti-Virus software. For customers who's policy requires AV software in any case, the TrendMicro software 'ServerProtect' can be used (see current release note).

CL-57 **OSO HX Server PC**	**Protect OpenScape Office HX Server /** **Suse Linux Enterprise Edition (SLES)**
Measures	• Automatic SLES update is activated at installation, for details [8] • Secure and confidential root password implemented • No user accounts in addition to the original settings • No changes e.g. additional open ports
Executed	Yes: ☐ No: ☐ Not part of solution ☐
Comments, Reasons, References	

8 Phones and Clients

HiPath 3000 supports several system and system independent phones and clients. Please observe the product-related security checklists and / or administration manuals.

Use released devices according to the current sales information only. For OpenStage HFA family, compare checklist [7].

It is recommended that the **administration** access to the devices be protected by individual passwords, if possible. Do not keep the initial value. For password policy, see also 9.1.

CL-58 System Phones	**Administration access protected by strong password (PIN)**
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	System-specific PIN ☐ device-specific PIN ☐

In addition, the **registration** of an IP device with HiPath 3000 / HG 1500 shall be protected by an individual password. This secures from bringing a new device with a known call number to the network taking the part of the original device. For password policy, see also 9.1.

CL-59 HiPath 3000 and HFA Devices	**HFA device registration password (option)**
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	System-specific PIN ☐ device-specific PIN ☐

For SIP devices, **authentication** must be used in HiPath 3000 / HG 1500 to protect against registration of unauthorized devices. This applies also to HiPath Cordless IP devices and SIP terminal adapters. Increasing SIP attacks may lead to toll fraud or service degradation.

CL-60 HiPath 3000 and SIP devices	**SIP device authentication activated (mandatory)**
Measures	• Authentication activated for all SIP subscribers with strong passwords (see 9.1) • An individual password is used for every device (so that not the whole system is corrupted if one phone is lost) • SIP User ID is different from call number (e.g. by using a system specific prefix)
Executed	Yes: ☐ No: ☐

Comments, Reasons, References	

9 Addendum

9.1 Password Policies

These are the recommended criteria for selection of passwords or PINs (numerical passwords). Please implement them unless other company specific rules are defined at customer site.

	Password	**PIN**
Minimal Length	8	6
Minimal number of upper case letters	1	-
Minimal number of numerals	1	PIN is numerical
Minimal number of special characters	1	-
Maximal number of consecutive identical characters (e.g. bbb, 333)	3	3
Maximal number of sequential characters in increasing or decreasing order (e.g. abc, 123, 987)	Password length - 3	PIN length - 2
Change interval (Maximum password age)	90 days	90 days
Maximum number of erroneous login attempts	5	5
Password History (number of recently used passwords, which are not accepted again)	5	5

Do not use trivial or easy to guess passwords. Do not reuse old passwords, at least from latest history. Take care that password entry cannot be observed and that no other persons can get access to them.

Currently there is no enforcement of these rules within HiPath 300, HG 1500, OpenScape Office HX and HiPath Xpressions Compact. All users have to be instructed to comply with password policies and are responsible for their observation.

9.2 References

[1] **HiPath 3000 Manager E Administrator Documentation**
available via e-Doku or SEBA Portal / product information
HiPath 3000 V9 product homepage

[2] **HG1500 V9 Administrator Documentation**
available via e-Doku or SEBA Portal / product information
HiPath 3000 V9 product homepage

[3] **OpenScape Office V3 Administrator Documentation**
available via e-Doku or SEBA Portal / product information
OpenScape Office V3 product homepage

[4] **HiPath 3000/5000 V9 Service Manual**
available via e-Doku or SEBA Portal / product information
HiPath 3000 V9 product homepage

[5] **Support of Operating System Updates for Server Applications**
http://wiki.siemens-enterprise.com/images/c/c0/Security_Policy_-_Support_of_Operating_System_Updates_for_Server_Applications.pdf

[6] **Support of Virus Protection Software for Server Applications**
http://wiki.siemens-enterprise.com/images/2/21/Security_Policy_-_Support_of_Virus_Protection_Software_for_Server_Applications.pdf

[7] **Security Checklist OpenStage V2 Phones**
https://enterprise-businessarea.siemens-enterprise.com/productinfo/document/Fz!Eyz-tRHM_/OpenStage%20SIP%20V2%20Installation%20Guide%20-%20Security%20Checklist.pdf

[8] **OpenScape Office HX / LX Server Guideline**
available via Wiki
http://wiki.siemens-enterprise.com/wiki/OpenScape_Office_HX/LX_Server_Guideline

[9] **OpenScape Office V3 Security Checklist**
OpenScape Office V3 product homepage

About Siemens Enterprise Communications:

Siemens Enterprise Communications is a premier provider of end-to-end enterprise communications solutions that use open, standards-based architectures to unify communications and business applications for a seamless collaboration experience. This award-winning "Open Communications" approach enables organizations to improve productivity and reduce costs through easy-to-deploy solutions that work within existing IT environments, delivering operational efficiencies. It is the foundation for the company's OpenPath commitment that enables customers to mitigate risk and cost-effectively adopt unified communications. This promise is underwritten through our OpenScale service portfolio, which includes international, managed and outsource capability. Siemens Enterprise Communications is owned by a joint venture of The Gores Group and Siemens AG. The joint venture also encompasses Enterasys Networks, which provides network infrastructure and security systems, delivering a perfect basis for joint communications solutions.

For more information about Siemens Enterprise Communications or Enterasys, please visit www.siemens-enterprise.com or www.enterasys.com

Siemens Enterprise Communications
www.siemens-enterprise.com

Siemens Enterprise Communications GmbH & Co. KG is a Trademark Licensee of Siemens AG

Hofmannstr. 51
81359 Munich, Germany

Status 07/2011