

Secure Communication with HiPath
“End-to-End” across your Company with Secure Real
Time Protocol (SRTP)
Frequently Asked Questions (FAQ)

Contents

1	Why is security growing in importance?.....	3
2	What are the downtimes and costs?.....	3
3	What threats exist?	3
3.1	Eavesdropping / interception	3
3.2	DoS attacks.....	3
3.3	Viruses and Trojan horses	4
3.4	Masquerade / unauthorized access	4
4	Are these threats possible with VoIP and other applications?.....	4
5	Which customer target groups require security and when?.....	4
5.1	Management / executive floor	4
5.2	Personnel department.....	4
5.3	Sales	4
5.4	Purchasing team / buyers	4
5.5	Development / research / production	5
6	Why do these target groups require security?	5
6.1	Management / executive floor	5
6.2	Purchasing team / buyers	5
7	What should the security solution be like?.....	5
8	Why is Siemens the ideal partner for security?.....	5
9	What types of security exist and what types will help with Voice over IP?	6
9.1	Securing buildings.....	6
9.2	Securing networks	6
9.3	Identity and access management for	6
9.4	Data traffic control management.....	6
9.5	Encryption for voice and data	6
10	What standards exist for VoIP end-to-end encryption?	6
11	What security measures are offered by the HiPath 3000 V6.0 and HiPath 4000 V3.0 communication platforms?.....	6
12	Why end-to-end security for VoIP with SRTP now?	7
13	How flexible is Siemens security?.....	7
14	What does this mean for individual Voice over IP users?.....	7
15	Does security work on a cross-location basis, even when system types vary?.....	8
16	How secure is this security?	8
17	What is the migration strategy for existing systems?.....	8
18	What administrative effort can be expected?.....	8
19	What does the HiPath Security Policy mean?	8
20	Summary.....	8

1 Why is security growing in importance?

Enterprises must adapt quickly to new situations if they are to rise above the competition in the marketplace. This requires enterprises to organize their work processes flexibly and build up a data network infrastructure in such a way that employees can access company resources at any time and from any location. In addition, data network interconnections between two companies are now state of the art. These can be data connections between headquarters and branches or between production and suppliers. Information can be accessed from Logistics or the website. Such business openness leads many attackers to gain access to these resources and to disrupt operations (processes), however. New horror stories of this kind appear regularly in the press. This is why enterprises must arm themselves against these attacks.

2 What are the downtimes and costs?

Statistical information* indicates the significance of security. The cost of security violations worldwide was measured in tens of billions of dollars in 2003.

Cost of information security violations in USA:

> 100,000 US Dollars	10% of enterprises
10,000 to 100,000 US Dollars	17% of enterprises

It should be noted that many security violations never become public, so that total costs are probably much higher.

Downtimes for servers, applications and networks in the USA due to security violations:

More than three days:	7% of enterprises
One to three days:	10% of enterprises
8 to 24 hours:	21% of enterprises

)* Source: IT Security 2003, InformationWeek

3 What threats exist?

3.1 *Eavesdropping / interception*

Spying and hacking of phone calls
ARP spoofing

3.2 *DoS attacks*

Exploiting of programming faults
Overloading services through the use of freely available tools
Result

An unprotected service or entity is overloaded, the application or entity is out of service on short-term or long-term basis

3.3 Viruses and Trojan horses

Destroy information on hard disks
Open backdoors to network resources

3.4 Masquerade / unauthorized access

- Access to resources
- Operation under false identity

4 Are these threats possible with VoIP and other applications?

The attacks mentioned in section 4 have an effect on:

- Every entity (PC, server, switch, router, IP phone)
- Every application (e-mail: Outlook, Lotus Notes; Internet website; SAP; operating systems MS 2000, XP; Voice over IP...)

5 Which customer target groups require security and when?

5.1 Management / executive floor

- strategic information on the future of the enterprise
- mergers & acquisitions
- alliances & cooperative partnerships

5.2 Personnel department

- Confidential information on employees (salary, profile, professional development ...)
- Personnel development for various departments

5.3 Sales

- Projects, customer information, market analyses

5.4 Purchasing team / buyers

- Price information / conditions (sales / purchasing)
- Price calculation for new products
- Discussion of sales and results with the management

5.5 Development / research / production

- Software, tests, patents

6 Why do these target groups require security?

6.1 Management / executive floor

- Strategic management decisions are confidential. Competition could exploit this information for its own purposes.
- Information on sales and profit figures indicate an enterprise's liquidity

6.2 Purchasing team / buyers

- Other suppliers receive information on competitors and can optimize their price calculations
- Competitors come to the market with a comparable project that is less expensive to implement
- Information on sales and profit figures indicate the liquidity of the enterprise.

6.3 Personnel department

- Confidential information is published
- Colleagues' salary details are published
- Development opportunities decline
- Unrest in the enterprise, performance declines

6.4 Development / research

- Superiority in innovation is lost
- Costs for research and development among competitors drop

7 What should the security solution be like?

The security solution should be tailored to the customer. The right resources should be positioned at the right place. A customer analysis should be carried out to ensure that potential dangers are identified.

Evaluate analysis together with the customer and subsequently draw up the appropriate security policy.

8 Why is Siemens the ideal partner for security?

Security is a question of trust and faith for the customer. The places importance on:

- partners who have been active in the market for a long time
- product-neutral advice
- optimum use of available resources
- outsourcing, operation of the solution

9 What types of security exist and what types will help with Voice over IP?

Security exists in a wide variety of areas. These include:

9.1 *Securing buildings*

- Entry with smart card access

9.2 *Securing networks*

- Routing and traffic control
 - Firewalls to the Internet / service provider

9.3 *Identity and access management for*

- Firewalls
- Teleworkers

9.4 *Data traffic control management*

- IDS
- IPS

9.5 *Encryption for voice and data*

- VPN
- SRTP

Protective measures encompass the whole network and accesses. Voice over IP is just one application in the network.

10 What standards exist for VoIP end-to-end encryption?

- SRTP (Secure Real-Time Transport Protocol, RFC 3711)
- AES (Advance Encryption Standard)
- TLS (Transport Layer Security)
- VPN (Virtual Private Network)

11 What security measures are offered by the HiPath 3000 V6.0 and HiPath 4000 V3.0 communication platforms?

- SRTP:
- End-to-end encryption of VoIP stations on HiPath 4000 (HG3530) and HiPath 3000 (HG1500)

- HiPath 4000 networking (HG3550-HG3550)
- Networking with HiPath 4000 and HiPath 3000 (HG3550-HG1500)
- HiPath 3000 networking (HG1500-HG1500)
- Teleworker connection via xDSL in the case of HiPath 3000 (HG1500)
- VPN:

12 Why end-to-end security for VoIP with SRTP now?

The further development of software and hardware has its advantages and disadvantages. Various spying tools are available as freeware via the Internet; attacks can target communications directly and voice payload in particular.

The external security of the networks is assured using firewalls. Access to the LAN is assured by means of VPNs and access control mechanisms. The renowned “Gartner Group” consultants report that 80% of attacks come from within enterprises. This means that it is necessary ensure communication within the enterprise.

Unlike Virtual Private Networks (VPNs), no additional hardware or software is required for encryption and decryption. Encryption and decryption take place on a decentralized basis at the physical end of the connection – in other words in the terminal – and are already included in the operating software. SRTP has a revolutionary mode of operation. Only the usable content of a data package is encrypted with the Advanced Encryption Standard (AES). The package’s header information, which contains the sender and addressee, is not affected by encryption. For this reason, no particular changes are required for routing in the network and this remains unimpeded. For this reason, there is no additional delay during transmission which would have a negative impact on voice quality.

13 How flexible is Siemens security?

One of the key arguments in favor of Voice over IP is flexibility and mobility within the enterprise. This function provides excellent support with SRTP for payload encryption and AES for signaling encryption because encryption begins at an endpoint and continues as far as the other endpoint.

A large number of terminals supports this encryption algorithm; the right terminal can therefore always be selected for the relevant purpose and working processes receive the best possible support.

Since HiPath security encryption is based on standards, implementation in the LAN poses no problems.

14 What does this mean for individual Voice over IP users?

Nothing changes for the user.

- Voice quality remains the same
- There is no interference
- Security is activated and administered in the system

15 Does security work on a cross-location basis, even when system types vary?

End-to-end encryption is activated for HiPath 3000 networking on a system-wide basis for all IP stations and IP networks.

Payload switching also works when encryption is activated.

The encryption for individual gateways (HG 3530, HG3550) can be activated in HiPath 4000. A mixed operation within a HiPath 4000 between secure and insecure gateways is possible. The IP voice connection between secure/insecure terminates at the relevant gateway and is connected by means of the system's coupling field. The line between secure stations and a secure gateway is thus always encrypted.

In the case of heterogeneous IP networking between HiPath 3000 and HiPath 4000, provided that security is activated on both switches, end-to-end encryption in the network also works on a cross-location basis.

16 How secure is this security?

Encryption standard AES with a key length of 128 bits for signaling and SRTP for the voice payload are deemed secure.

17 What is the migration strategy for existing systems?

The fundamental requirement is HiPath 3000 V6.0 and HiPath 4000 V3.0 so as to achieve end-to-end security encryption. The system upgrade is normally based on the software.

The hardware can continue to be used (depending on the version). A Comscendo security license is available for security purposes. The licenses relate to IP stations (HG 1500, HG3530) and B channels for IP networking (HG1500, HG3550).

18 What administrative effort can be expected?

Terminals and switches are still administered with the management tools.

The DLS is used for security enhancements. The DLS handles the central administration of security for the relevant components.

19 What does the HiPath Security Policy mean?

- Provision of a HiPath security process throughout the HiPath organization to the customer
- Responsible employees in product management and development for HiPath security
- Cooperation with the CERT organization
- Internal security organization for product and system tests
- Interface to the local sales organization, in particular to consulting and service with patch management

20 Summary

- Development of a holistic perspective, define security as a cross-organizational task
- Identification of potential threats and understand preventive methods. Personnel are often the weakest link in the security chain
- Careful analysis of risks and initiation of the definition of security requirements
- Systematic evaluation of the existing security precautions

- Definition of a robust security policy (incl. rules, risk vs. investment, security management processes etc.)
- Drafting of a realistic plan to secure the network infrastructure
- Assessment of the key advantages and disadvantages of various VoIP scenarios, e.g. campus VoIP, trunking, IP-WAN and connections provided by Internet service providers, WLAN
- Use of existing expertise in relation to IT security
- Evaluation of offers from product and service providers who have comprehensive, practical experience, e.g. Siemens
- Setting up of event-controlled security management
- Improvement of awareness of security throughout the enterprise and communication of the effects of failure to observe the enterprise's security policy
- Definition of worst case scenarios and preparation for the worst case
- Awareness of the continuous imbalance between threats and the corresponding prevention.