Development of SSH Compliant UPS Management Products

Yutaka Katoh Shinji Kondoh Kouichi Hayashi Hironori Ogihara

1. Introduction

Our company has developed a variety of UPS management products to meet complex network environment and varied market needs, including the LAN interface card*1 and SANUPS T*2.

The LAN interface card and SANUPS T use Telnet protocol to perform computer shutdown, configure device settings, monitor the UPS state, and handle other operations. However, the information floating on the network with Telnet protocol is completely uncoded plain text, leaving the information open to the following types of attack from malicious hackers:

- Leakage of account or password information from stolen data
- Data leakage due to identity theft

Recently, many companies have realized the importance of protecting against these kinds of attacks, and UNIX and Linux computers are switching from Telnet protocol to SSH*3 protocol for the increased security features.

Looking at these trends, our company introduced SSH protocol into the UPS management products and developed a product that uses SSH protocol to perform computer shutdown, configure device settings, monitor the UPS state, and handle other operations.

This document introduces the features of the SSH compliant LAN interface card and SANUPS T.

*1: Yutaka Katoh and others: Development of LAN Interface Card "SANUPS" PRASD04
Refer to SANYODENKI Technical Report No. 18.

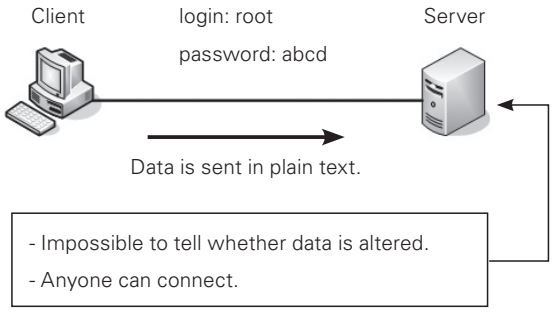
*2: Yutaka Katoh and others: Development of Power Manager "SANUPS T"
Refer to SANYODENKI Technical Report No. 20.

*3: Abbreviation for "Secure Shell".

2. What is SSH?

SSH is a program or protocol that allows a user to login to another computer via a network or enter commands into another machine from a remote location. It can be applied to the same operations as Telnet, but the biggest difference between SSH and Telnet is that the data on the network is encoded with SSH (Fig. 1).

＜With Telnet＞



＜With SSH＞

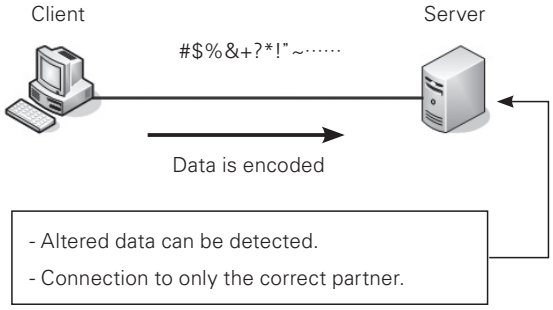


Fig. 1: Differences between Telnet and SSH

With Telnet, the login account and password are sent uncoded over the network, so there is a possibility that it could be intercepted by a third party and used by hackers. SSH, on the other hand, encodes all of the data over the network, including the login account and password, thus preventing information leakage.

Furthermore, two types of authentication are used between the server and the client when the client logs into server under SSH to preserve higher security.

- Host authentication: Verifies whether the server is the server that the user wants to login to.
- User authentication: Verifies whether the user is entitled to login to the server.

Host authentication and user authentication (when using public key authentication) require a "key" that uses anywhere from several dozen to 2,000 bits of data. A pair of keys, a private key and a public

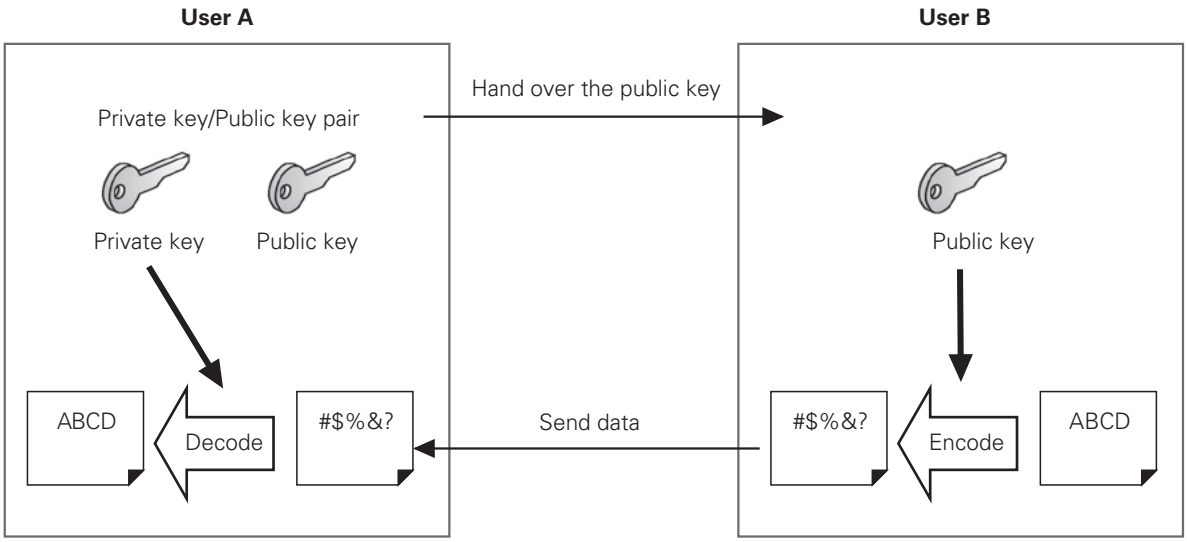


Fig. 2: Public key encoding method

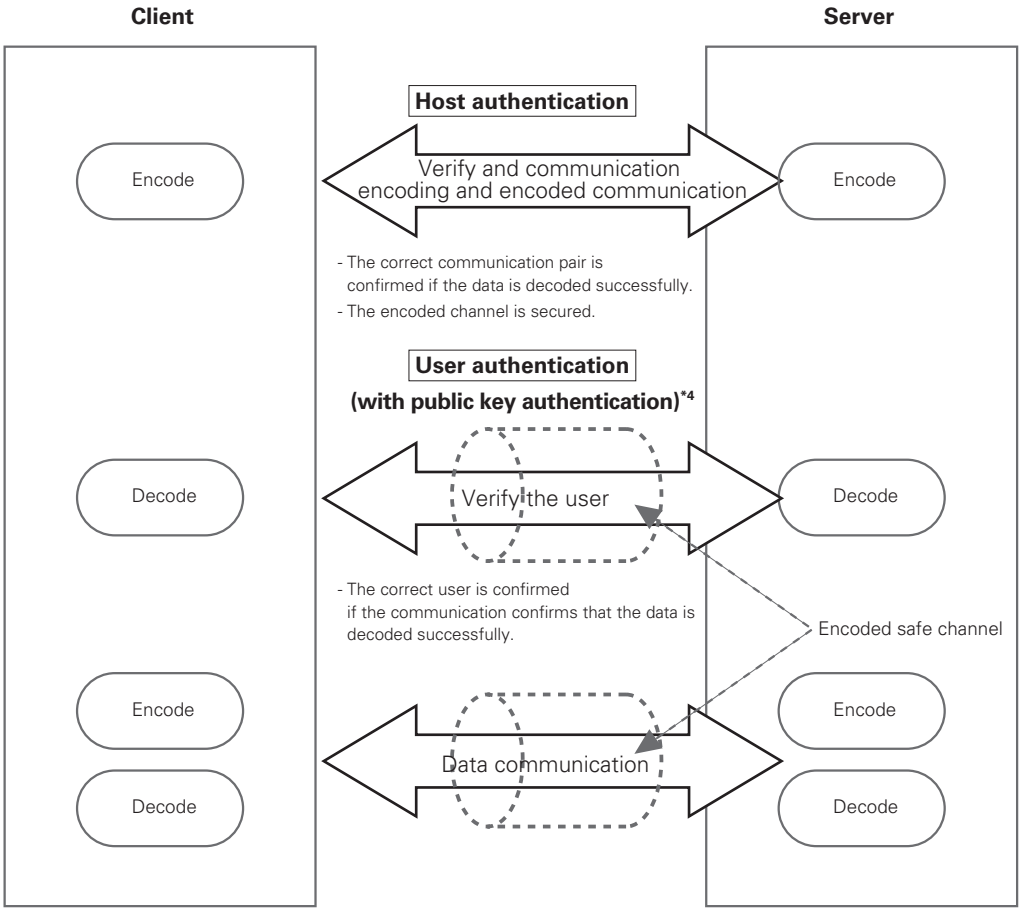


Fig. 3: System for SSH authentication and encoded communication

*4: When performing password authentication, the account and password are transmitted over the encoded channel.

key, is generated by a key generation program. Data encoded by a public key can only be correctly decoded by the corresponding private key (Fig. 2).

The server machine and client machine are registered so that one machine has the private key, while the other has the public key. Therefore, only a client with a pair of keys can login to the server.

The following steps are used for SSH communication. The general flow of SSH is shown in Fig. 3.

Step 1. Host authentication
The client checks whether the channel connects to the correct server. This step also secures the encoded channel.
Step 2. User authentication
The server checks whether the user has the right to login, and if login is permitted, the client is logged into the server.
Step 3. Data communication
Data is transmitted over the encoded channel.

The SSH specifications compliant with this development are shown in Table 1.

3. System configuration

The SSH compliant UPS management products that have been developed are as follows:

- LAN interface card (100Base-Tx)
- SANUPS T

The system configurations used for each product are shown in Fig. 4 and Fig. 5.

4. Features

4.1 Computer shutdown with SSH protocol (SSH client function)

When performing computer shutdown from the LAN interface card or SANUPS T, SSH protocol has been added to the conventional Telnet protocol in order to perform computer shutdown (① in Figs. 4 and 5).

When performing shutdown with SSH protocol, the procedure is the same as when using Telnet protocol. By defining the shutdown command in a script, the computer can be shut down. But unlike when performing shutdown with Telnet protocol, the SSH authentication settings must be configured. One of the following methods can be selected for SSH authentication based on the security level and processing time.

- Host authentication (yes/no)
- User authentication method (password authentication/public key authentication)

Fig. 6 shows an example of SSH authentication settings on a Web screen.

When using the LAN interface card, up to 8 devices can be shut down using SSH protocol.

4.2 Device settings with SSH protocol (SSH server function)

With a conventional terminal function, serial or Telnet protocol could be used to configure a device or monitor the UPS state, but now the SSH protocol can also be used to perform these same functions (② in Figs. 4 and 5).

This means that the LAN interface card of SANUPS T can safely be used to perform functions such as configure settings or monitor UPS even under environments that only accept SSH protocol as the security feature.

Table 1: SSH specifications

Item		Specifications	Remarks
SSH version		Version 2	
User authentication		Password authentication	Authentication using a password registered ahead of time by the user
		Public key authentication	Authentication using a private key/public key pair registered ahead of time by the user
Key conditions			
	Key format	OpenSSH format	
	Public key encoding method	DSA	Digital Signature Algorithm. Encoding method issued by the NIST (National Institute of Standards and Technology)
		RSA	Encoding method developed by Ronald Rivest, Adi Shamir, and Leonard Adleman
	Pass phrase	None	
	Key comment	None	
	No. of bits	1024	

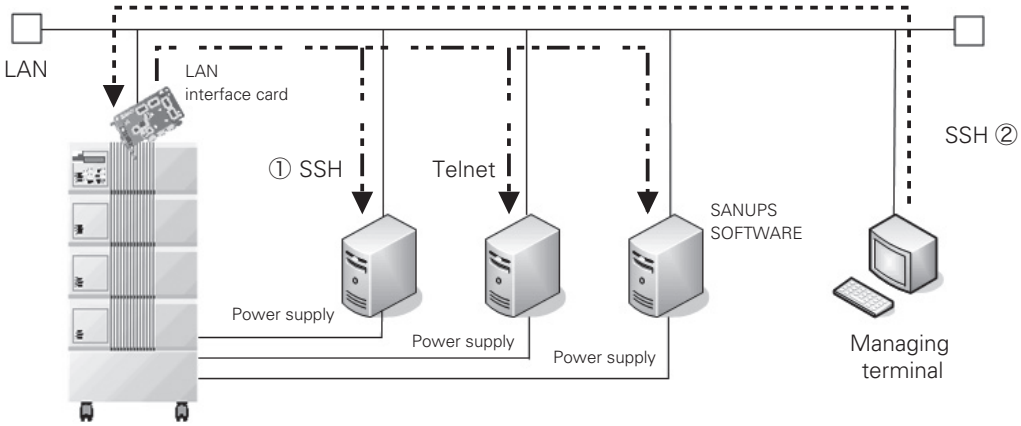


Fig. 4: LAN interface card system configuration

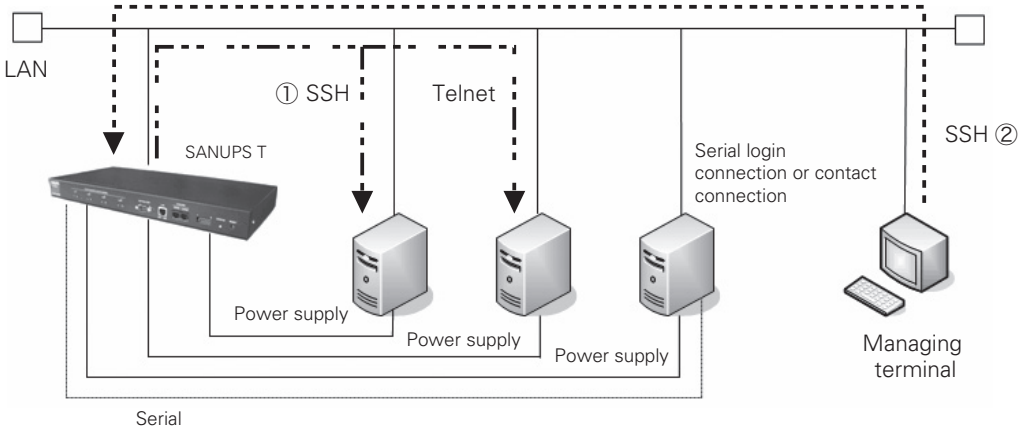


Fig. 5: SANUPS T system configuration

＜When using password authentication＞

＜When using public key authentication＞

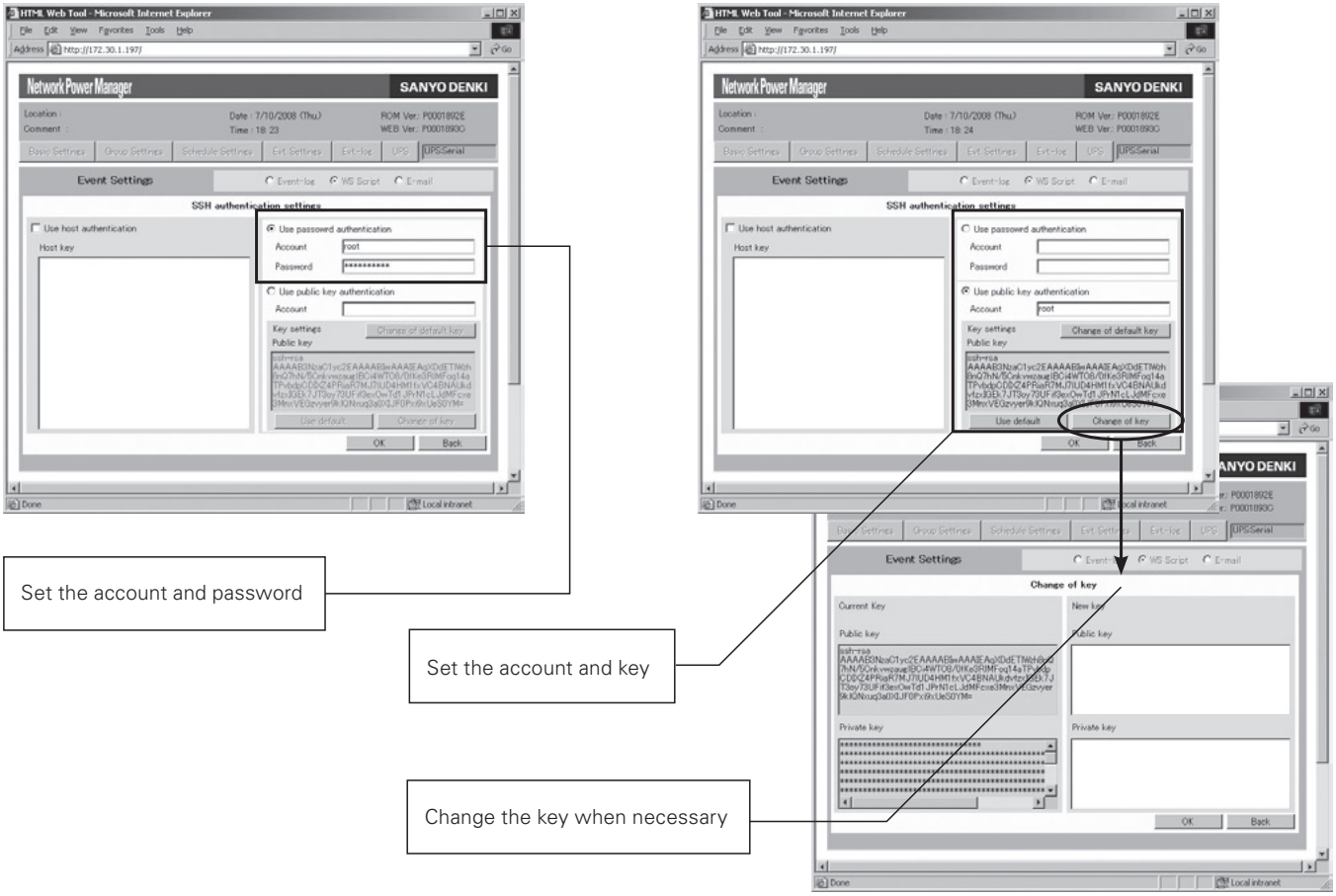


Fig. 6: Example of SSH settings through Web on SANUPS T

Table 2: Functions of a general user account

Item \ Device	LAN interface card	SANUPS T
Connection device/output status display	Yes	Yes
Register/change/delete device	No	No
Network information settings	Display only	Display only
Control time settings	Display only	Display only
Service settings	No	No
Account settings	No	No
Email settings	No	No
Schedule settings	Display only	Display only
Clock settings	No	No
Event settings	No	No
State/measurement value display	Yes	Yes
Event log display	Yes	Yes
Control	No	No
UPS information display	Yes	Yes
Output group settings		Yes

4.3 Addition of other functions

4.3.1 Support for general user accounts

With conventional UPS management products, only management level accounts were available. When this account was used to log in with a UPS management project, operations such as device settings, status display, and controls could all be performed (② in Fig. 4 and Fig. 5). Therefore, maintenance engineers who were not managers could only monitor the UPS state, so maintenance engineers had to be given access to management accounts. In this situation, all of the workstation login information (including account and password) were open to the maintenance engineer, thus causing possible security problems. As a solution to this problem, a general user account has been added. This account allows the user to perform actions such as monitor the UPS state and manage the functions in a truncated format.

Table 2 shows the list of functions available when logged in with a general user account.

4.3.2 Strengthened the email sending function

In addition to the UPS state and measurement value used with the conventional product, more information has been added to the email sending function, including UPS type, battery test results, and battery life.

5. Conclusion

These products were developed with security in mind. By using SSH protocol version 2 that is already employed by other companies, our company is able to submit our attitudes towards security to society.

We hope that we will be able to use this development as a way to become a more trustworthy company with heighten awareness of security issues.

Documentation

(1) Daniel J. Barrett, et al.: SSH, The Secure Shell: The Definitive Guide

(2) Yusuke Shinyama: Introduction to Open SSH

Yutaka Katoh
Joined Sanyo Denki in 1991.
Power Systems Division, 2nd Design Dept.
Worked on the development and design of power supply equipment and power supply management systems.

Shinji Kondoh
Joined Sanyo Denki in 1985.
Power Systems Division, 2nd Design Dept.
Worked on the development and design of power supply equipment and power supply management systems.

Kouichi Hayashi
Joined Sanyo Denki in 1997.
Power Systems Division, 2nd Design Dept.
Worked on the development and design of power supply equipment and power supply management systems.

Hironori Ogihara
Joined Sanyo Denki in 2005.
Power Systems Division, 2nd Design Dept.
Worked on the development and design of power supply equipment and power supply management systems.