Type 33 Star Army Communications Network Encryption System

The Type 33 SACN Encryption system, was developed to counter the threat posed by the terrorist group Independent Worlds League. It became available in YE 33.

The SACNES affects all PANTHEON systems, all devices designed to interface with it, and all NH-series life forms that require access.

Electronic Security

The system adds multiple levels of security and access control. Part of the security system depends on the fact that each quantum computer has its own signature, an electronic fluctuation that can be detected. The Uncertainty principle ensures that no two quantum computers will ever have the same signature.

Any computer that has not been equipped with the SACNES is considered an untrusted system; this limits the level of access it is given to trusted systems.

The encryption of the system uses a fractal encryption code that is modulated by the IES's unique quantum signature. This means that each IES system has its own unique encryption. When a system is upgraded, its data is uploaded to the largest IES system in the area. From there its status as a trusted system spreads across the network.

Authentication process is done by vetted Kessaku Systems trained Star Army Information Technology specialists. They use trusted Isolated Computer Pad, that are equipped with self destruct if attempted to be operated by anyone other than the issued person.

Authentication

One new aspect of the security is that all trusted systems, and personnel must check in periodically.

Computers check into the network between every 5-7 minutes. This is essentially a ping that sends to the senior system, the ping consists of the ID, location and status of the IES. This means that the network monitors the location of every operating IES. This was added so that in the unlikely event that someone tried to duplicate a systems encryption it would be flagged as coming from a different location and rejected. When the system pings it also sends when it will ping again. Should an IES fail its ping it is put into yellow status. If a system fails to ping within 84 minutes it is flagged as Red/Untrusted.

Soldiers

All active duty Star Army of Yamatai NH-Series lifeforms require an upgrade to install a SACN Access

Nodule.

Authorization

Information and communications have the standard classifications. But an additional qualifier has been added. Previously anyone with the proper security could access any data that it allows. The new Authorization restricts data to persons who have a job required need to access.

Example: Previously orders for a fleet to prepare could be monitored by any soldier in the vicinity. Now such communications is limited to command staff of the ships in question, and their upward chain of command.

Untrusted Access

An untrusted system cannot access secure systems. They can access insecure levels, however any data transfer initiated by an Untrusted system is shunted to an isolated storage device. It is then scanned and analyzed for potential threats.

Status

Access Status falls into the following categories.

IES			
Color	**Status**	**Reason**	**Corrective Measures**
	Trusted	Compliant	
	Watched	Missed 1-11 pings	Must reconnect and provide accounting
	Limited	Missed 12+ pings	Must be checked by authorized technician prior to regaining trusted status
	Untrusted	Reported hostile boarding	Must be checked by authorized technician prior to regaining trusted status
	Untrusted	Reported being boarded by hostile and accessed.	Ship must surrender, if resists capture if possible, or destroy if no alternative