Overview of DNP3 Security Version 6

What is it?

Starting in the fall of 2020, the DNP3 Security methodology consists of two separate protocols, as illustrated in Figure 1 and Figure 2:

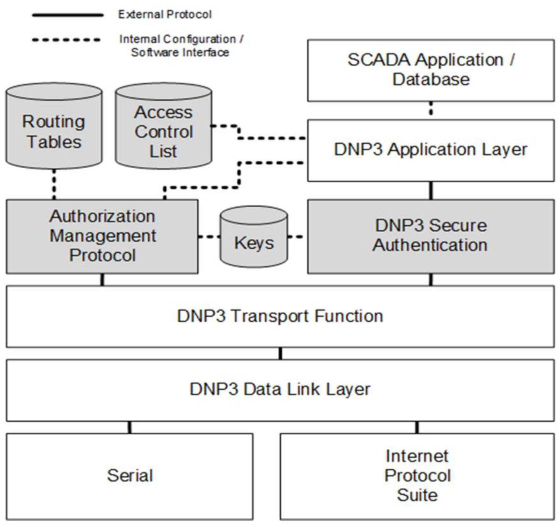


Figure 1. DNP3 Security Architecture

DNP3 Secure Authentication (DNP3-SA) is a separate protocol layer introduced between the DNP3 Application Layer and the DNP3 Transport function, as illustrated in Figure 2. As in previous versions, DNP3-SA uses Message Authentication Codes (MACs) to provide the capabilities of a secure communications session including **authentication** ("Are you who you say you are?") and message **integrity** checking ("Has the message been tampered with?"). It provides semi-automated device **enrollment** including generation of cryptographic **keys**, as discussed later in this summary. *Because DNP3-SA is now a separate layer, it could be used by protocols other than DNP3.*

The Authorization Management Protocol (AMP) is a new protocol used together with the DNP3 Application Layer and DNP3-SA to centrally manage which devices are authorized to communicate. Since DNP3 devices may not have access to network layer communications, AMP builds its own **routing tables** to direct messages between masters, outstations and a central Authority. AMP may be used to perform role-based access control (RBAC), in which case it informs the outstation of which roles and corresponding permissions the Authority assigns to particular masters. Optionally, **Access Control Lists (ACLs)** may be configured on the outstation to enforce permissions at a per-point level.

As with all DNP3 communications, DNP3 security protocols may operate over either serial links or Internet protocol suites.

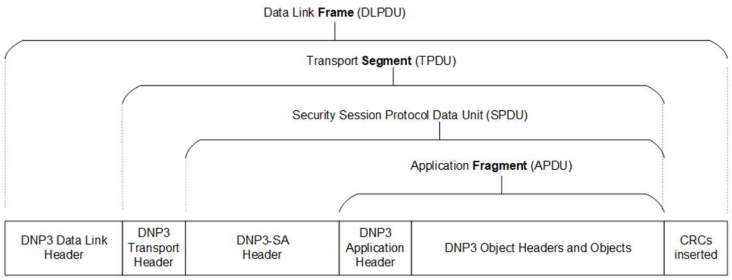


Figure 2. DNP3 Security Protocol Layers & Terms

Why a New Version?

In general, the new version of DNP3 security greatly reduces the overall complexity of the design, which makes implementations less costly and reduces the possible number of attacks. The new version:

- Addresses the vulnerabilities that were identified in DNP3 Technical Bulletin TB2016-002.
- Removes the multi-user feature, which added too much complexity without providing additional security.
- Eliminates the Challenge / Reply sequence because it creates too much overhead and complicates the DNP3 initialization sequence.
- Removes the need to use both a sequence number and random challenge data to protect against replay attacks, and as a result eliminates complications and potential attacks arising from both the master and outstation updating sequence numbers.

- Removes the “key status request” at the start of session initialization that had introduced some vulnerabilities.
- Adds version identification at initialization time to help with backward-compatibility.
- Adds new algorithms, e.g. BLAKE2, SHA-3, elliptic curves (low overhead)

New Capabilities: Encryption, Enrollment and Centralized Authorization

The new version of DNP3 security adds three new capabilities.

Firstly, in response to many requests, DNP3-SA will now support simultaneous authentication and **encryption** of data for confidentiality. The algorithm used will be AEAD-AES-256-GCM, which is used by TLS 1.2 and found in open security software packages. It will still be possible to use DNP3-SA using authentication only, and many utilities may prefer to operate in this mode for troubleshooting purposes.

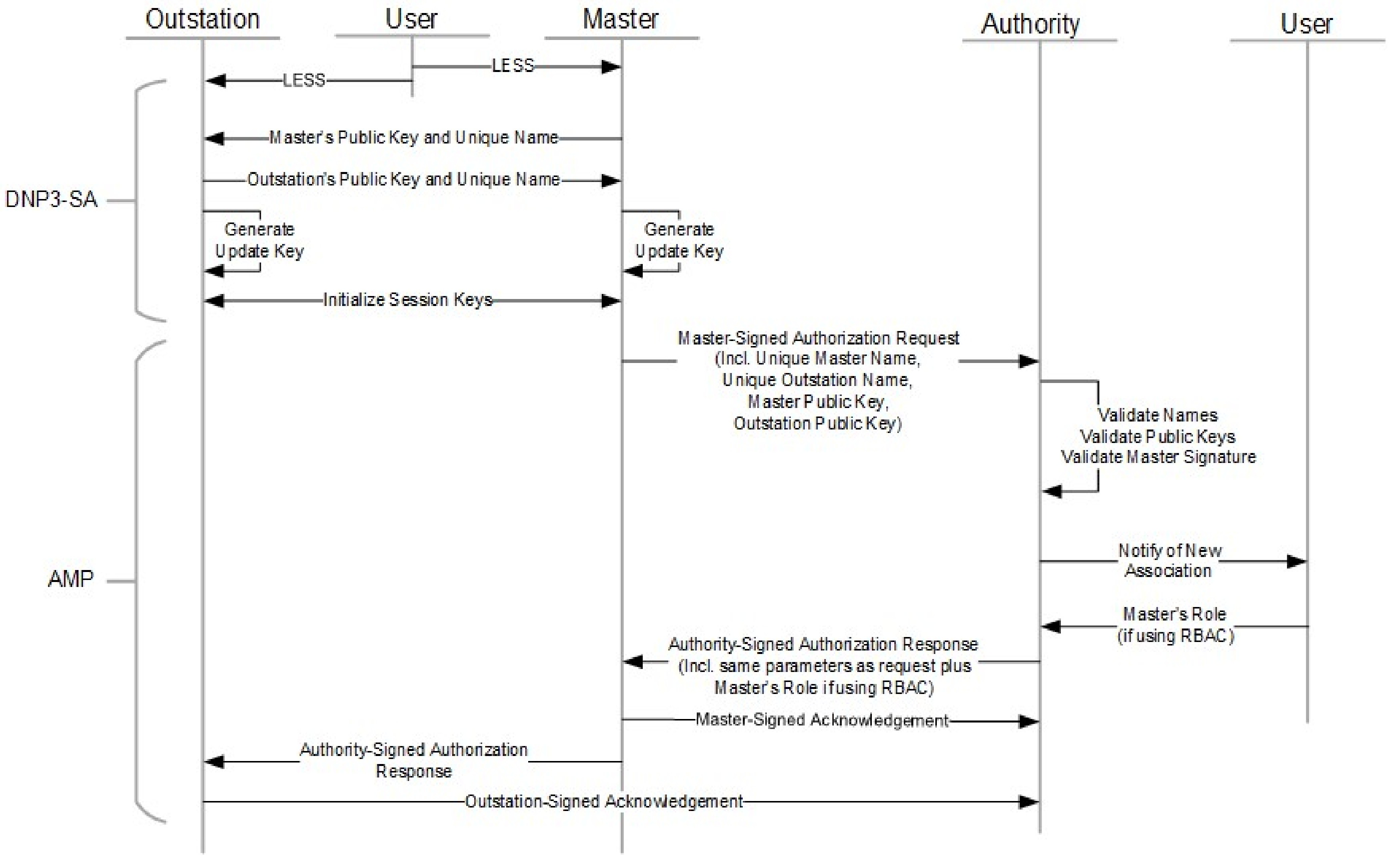
Secondly, as shown in Figure 3,in DNP3-SAv6, the Update Key is initialized using a **“device enrollment”** process in which the Update Key is never known by, or presented to a person. This mechanism avoids the following problems which could occur if, instead, the keys were preshared:

- Pre-sharing is prone to errors because keys are typically long strings of digits which are difficult for people to remember.
- Pre-sharing encourages people to write down the key, and/or exchange the key via risky external mechanisms such as email.
- Pre-sharing is risky because it requires a person to know the key, and any person may inadvertently disclose it, or become an attacker.

In the enrollment process, a human user provides a Low-Entropy Shared Secret (LESS), essentially a one-time-use password, to approve and commission the communications between the two devices.

Lastly, the addition of AMP provides an optional **centralized authorization** mechanism in which a person, through a system called an Authority, approves the connectivity and RBAC roles permitted for each pair of devices in the system, *after* the devices have generated their keys.

Figure 3. Enrollment and Authorization


Outstation
User
Master
Authority
User
LESS
LESS
Master's Public Key and Unique Name
Outstation's Public Key and Unique Name
DNP3-SA
Generate Update Key
Generate Update Key
Initialize Session Keys
Master-Signed Authorization Request (Incl. Unique Master Name, Unique Outstation Name, Master Public Key, Outstation Public Key)
Validate Names
Validate Public Keys
Validate Master Signature
Notify of New Association
AMP
Master's Role (if using RBAC)
Authority-Signed Authorization Response (Incl. same parameters as request plus Master's Role if using RBAC)
Master-Signed Acknowledgement
Authority-Signed Authorization Response
Outstation-Signed Acknowledgement