SYBASE®

Sybase® IQ Advanced Security Option

Protecting your valuable data assets without sacrificing flexibility

AT A GLANCE

- FIPS Transport Layer Security protects your data by securing client-server communications

- IPV6 support provides additional security while adding flexibility

- Kerberos authentication enables secure single login

- Column-level encryption adds flexibility and precision to database security.

TAKING SECURITY TO THE NEXT LEVEL

The Sybase IQ Advanced Security Option provides the highest levels of security capability for Sybase IQ environments. For data in-flight, this option enables encryption of client-server communication and supports the IPV6 protocol. For data at rest, the Advanced Security Option allows user access with authentication against Kerberos servers, supports FIPS 140-2 certified algorithms, and provides for strong AES compliant encryption of data stores at the column, table, or database level.

PROTECTING DATA AT REST

Kerberos is an authentication protocol which ensures mutual authentication between clients and servers over any network connection. In other words, this feature allows maintenance of just a single login ID for both Sybase IQ connections and operating systems and/or network logins. The Kerberos credentials can be used to connect to Sybase IQ without specifying a user ID password. With Kerberos in place, your Sybase IQ environment is protected from eavesdropping and other malicious (or unintended) exposure or interference.

FIPS 140-2 certification means that Sybase IQ provides encryption compliant with the Federal Information Processing Standard 140-2 approved encryption technology. Frequently mandated by government agencies and vendors who work closely with them, FIPS 140-2 is a set of standards for cryptography modules which include both hardware and software components. Compliance with FIPS 140-2 ensures an analytics environment that is highly secure and that can interoperate securely with other entities driven by the same set of standards. A non-deterministic approach to encryption mandated by FIPS 140-2 ensures the highest levels of security whereby the same input data when encrypted with a given key yields different output formats every time, yet it can be decrypted using the key. Via the Advanced Security Option, Sybase IQ supports FIPS compliant encryption on all supported platforms.

Column-level encryption adds flexibility to security by enabling you to customize security levels within a single database. The option to encrypt one or more columns makes it possible for multiple sets of users, having different needs for data access, to work from the same database without risk of exposure of sensitive data to users who should not have access to it. Sybase IQ supports explicit user encrypted columns using ENCRYPT and DECRYPT functions that are callable from within the application.

PROTECTING DATA IN-FLIGHT

The Advanced Security Option extends Sybase IQ's support of transport layer security (TLS). Similar to the Secure Sockets Layer, TLS is an encryption protocol above TCP/IP in the network stack. While the Sybase IQ Enterprise edition provides native support for Free RSA encryption for TLS, the Advanced Security Option adds FIPS-certified RSA.

Support for the IPV6 protocol adds simplicity and flexibility, as well as security, to your Sybase IQ environment. The larger address space of IPV6 avoids address space exhaustion, and eliminates the need for network address translation. This greatly simplifies network administration. Moreover, IPV6 support includes IPSEC, a mandatory component of IPV6 which secures internet protocol communications by authenticating and encrypting each IP packet of a data stream.
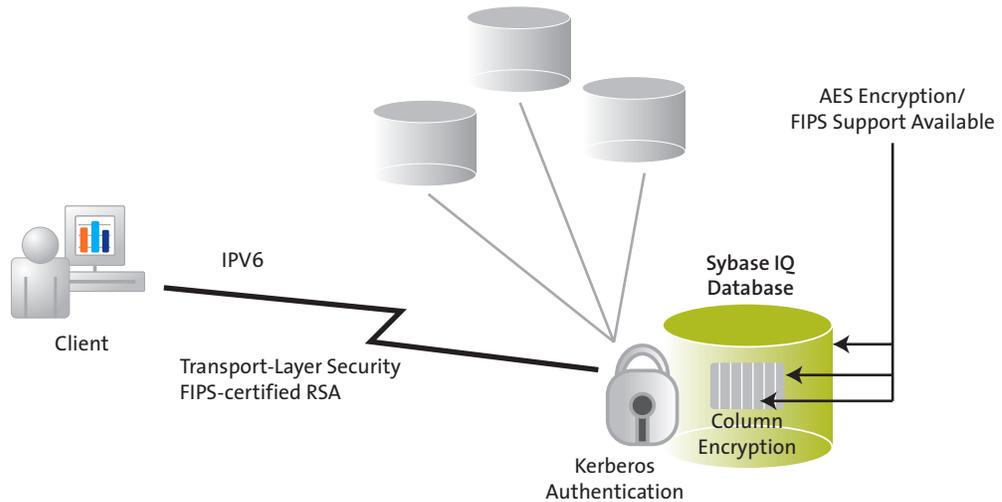
Figure 1: The Sybase IQ Advanced Security Option provides heightened security for your Sybase IQ by protecting data in flight or at rest. For data in flight, FIPS Transport Layer Security protects your data by securing client-server communications. Support of the IPV6 provides additional security to in-flight data while adding flexibility. For data at rest, Kerberos authentication enables secure single login. Column-level encryption adds flexibility and precision to database security. Plus, FIPS-compliant encryption can be applied at the table, database, or column level.

ABOUT SYBASE IQ

Sybase IQ is the world's leading column-based analytics server, designed specifically to deliver faster results for mission critical analytics and reporting solutions on standard hardware and operating systems. It works with diverse data—including unstructured data—and diverse data sources to deliver unsurpassed query performance at the lowest price/performance available.

SYBASE®