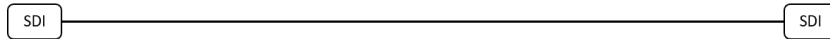
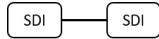


SDI-3 or OTO SDI

Imagine two SDI controllers that are paired when in physical proximity, and then they can be set apart and maintain a secure connection for as long as needed. Even keys can be rotated at a distance as often as needed. SDI-3 maintains the same grade of cryptographic strength throughout the duration of the connection. It can go dormant and resume connection at a long distance.



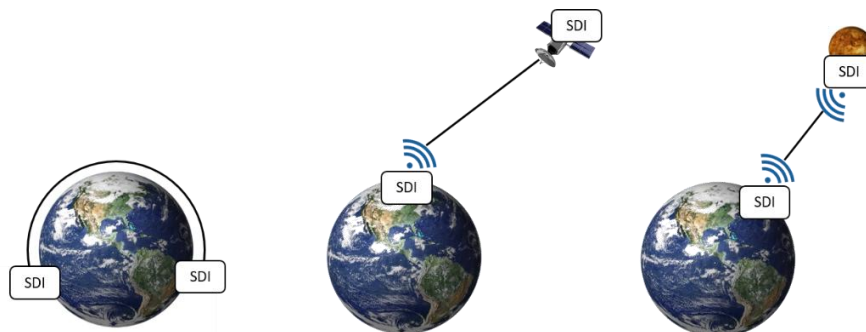
The connection between two SDI-3 controllers can be interrupted, like by jamming signal, but not cut through to intercept the content.



SDI-3 messages can safely traverse multiple domains and don't depend on URLs. They can run through any kinds of messaging media without the possibility of being compromised. They can be lost, but not breached.



They can travel very long distances as long as the media transporting them can handle. If a message reaches wrong destination, it is lost but not compromised.



In conclusion, SDI-3 messages are secure digital containers that can be attached to any kind of routing system, like the Internet, cellular network, email, SMS, direct wireless or wired connection, etc. Each message contains small amount of data (directive) and cryptographic authentication information (nonce), though it is not designed to transport large amounts of data, but deliver authentication information.