

specifications. In establishing the Technical Framework for the DoD PKI, the DISA and NSA plan to fully integrate both the requirement for interoperability with federal and commercial PKIs, and the capability to outsource some or all DoD PKI services.

Although it embraces relatively "low-assurance" transactions, the Defense Travel System (DTS) requires integrity and/or authenticity services provided by digital signature. To be interoperable, both to DoD entities and with the private sector organizations, the DTS will support both DSS and RSA signatures. As the first step in establishing a DoD-wide PKI service, the DISA, with support from NSA, will enable a PKI for DTS efforts in Defense Travel Region Six as a starting point for using PKI services throughout the DoD. This initial service complements the "high-assurance" PKI services being established by the NSA and DISA to protect and provide access control for classified information.