Certificates in the Internet: State, Issues, and Futures

Abstract: This presentation examines current progress, issues, and future directions in IETF work on Internet certificate usage. A certificate profile and operational protocols have been published. Current topics include high assurance qualified certificates, management protocol alternatives, application integration (e.g., S/MIME, IPsec), time stamping, and attribute certificates for authorization.

Andrew Nash
Director, PKI Technologies and Standards
RSA Security, Inc.