

PDF/PGP Verification

Many organizations provide PKI based verification services for authenticity and integrity of PDF documents, to comply to legal and regulatory requirements. X.509 is the “de facto” standard for this security measure.

Although some organizations have a self imposed X.509 policy, most organizations are either not aware of security issues, or are deterred by PKI requirements, that include third-party Certificate Authorities (CAs), Time Stamping Authorities (TSAs), and PDF signature-compliant PDF readers.

PDF/PGP Verification offers a simple PGP based PKI alternative. The PDF document is created with the detached PGP signature included as comment. The PDF is verified by stripping and decoding the comment as PGP detached signature, and using it to verify the integrity of the remainder PDF.

Any organization can offer a Public PDF/PGP Verification Service on a trusted SSL Secured Web Site, and add a tailored URL link to this site in their PDF/PGP signed documents. As the service has access to the PGP public key of trusted signers, authenticity and integrity of uploaded PDF/PGP files can be verified.