ABSTRACT

A terminal (40a) comprises: a revocation number verification unit (435) that obtains a revocation number from a repository (20) storing such revocation number that is information serving as a criterion for judging the validity of a server certificate (75); a revocation number storage unit (436) that stores the obtained revocation number; a certificate serial number extraction unit (437) that reads out, from the server certificate (75), an identification number for identifying such server certificate (75); a revocation judgment unit (438) that judges the validity of the server certificate (75) b y comparing the read-out identification number with the revocation number stored by the revocation number storage unit (436); and a communication unit (420) that establishes a communication with an application server (30a) when the server certificate (75) is judged valid, and does not establish a communication with the application server (30a) when the server certificate (75) is judged invalid.