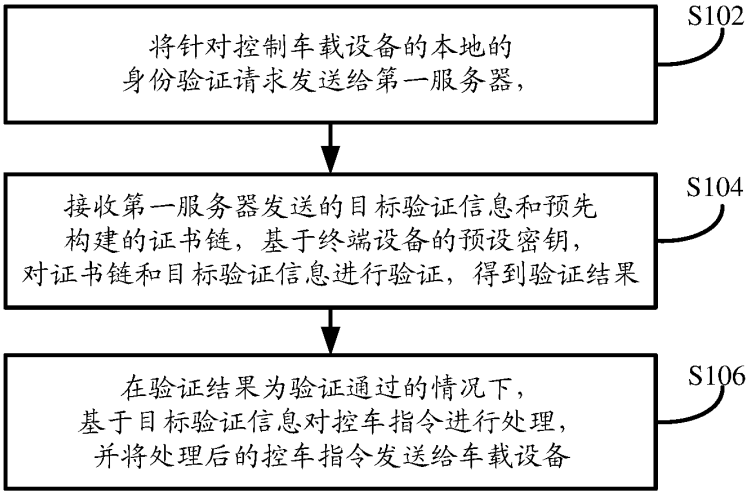

将针对控制车载设备的本地的
身份验证请求发送给第一服务器，
S102
接收第一服务器发送的目标验证信息和预先
构建的证书链，基于终端设备的预设密钥，
对证书链和目标验证信息进行验证，得到验证结果
S104
在验证结果为验证通过的情况下，
基于目标验证信息对控车指令进行处理，
并将处理后的控车指令发送给车载设备
S106

图 1A

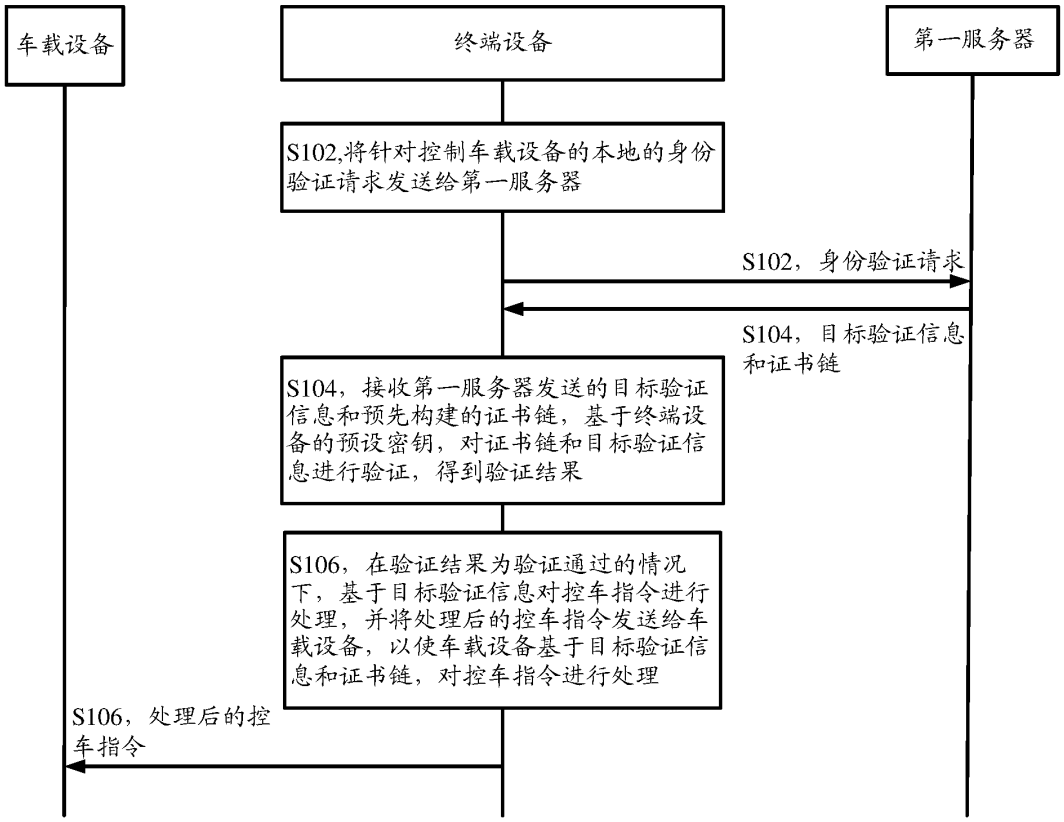

车载设备
终端设备
第一服务器
S102,将针对控制车载设备的本地的身份验证请求发送给第一服务器
S102，身份验证请求
S104，目标验证信息和证书链
S104，接收第一服务器发送的目标验证信息和预先构建的证书链，基于终端设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果
S106，在验证结果为验证通过的情况下，基于目标验证信息对控车指令进行处理，并将处理后的控车指令发送给车载设备，以使车载设备基于目标验证信息和证书链，对控车指令进行处理
S106，处理后的控车指令

图 1B

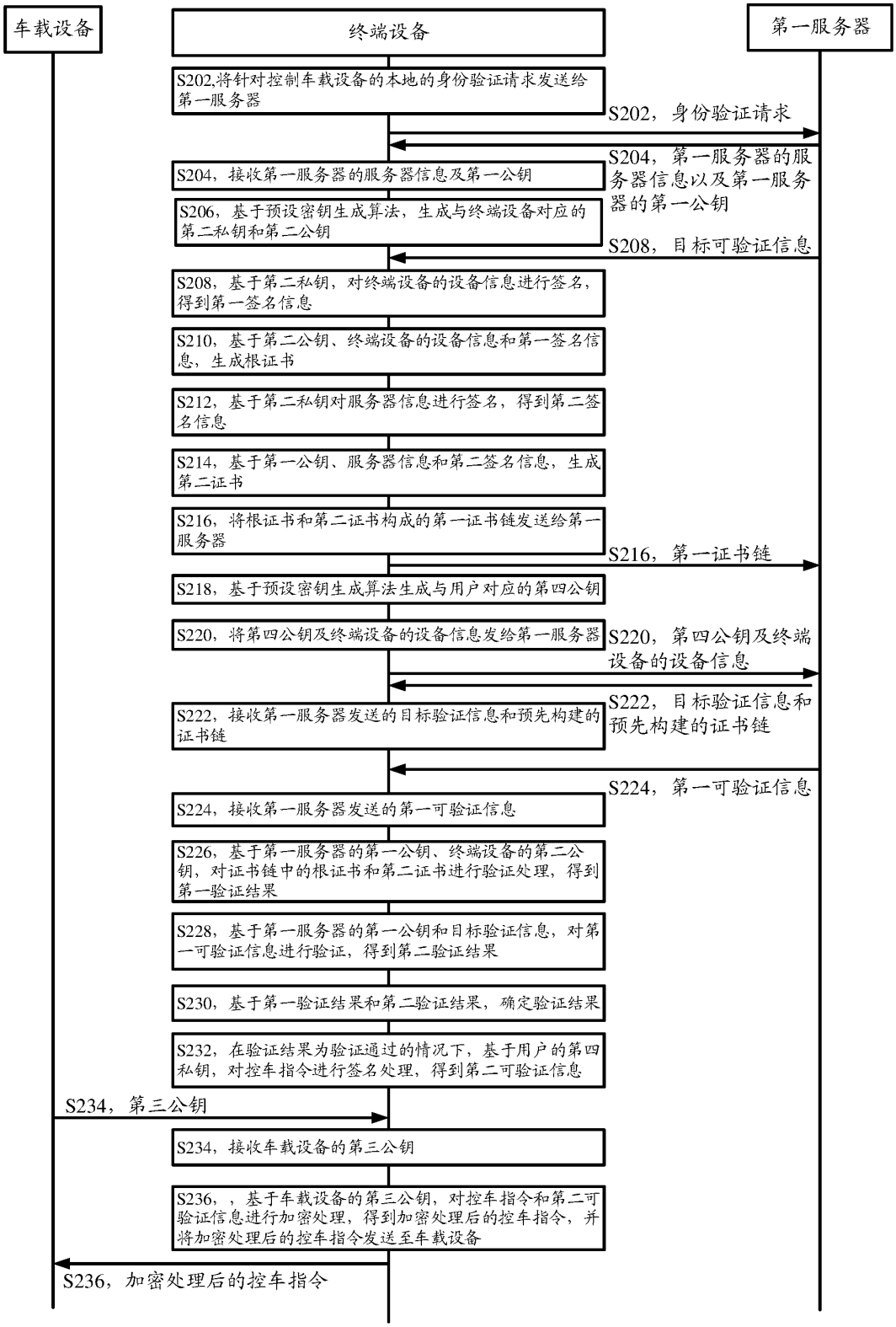

车载设备
终端设备
第一服务器
S202,将针对控制车载设备的本地的身份验证请求发送给第一服务器
S202，身份验证请求
S204，接收第一服务器的服务器信息及第一公钥
S204，第一服务器的服务器信息以及第一服务器的第一公钥
S206，基于预设密钥生成算法，生成与终端设备对应的第二私钥和第二公钥
S208，目标可验证信息
S208，基于第二私钥，对终端设备的设备信息进行签名，得到第一签名信息
S210，基于第二公钥、终端设备的设备信息和第一签名信息，生成根证书
S212，基于第二私钥对服务器信息进行签名，得到第二签名信息
S214，基于第一公钥、服务器信息和第二签名信息，生成第二证书
S216，将根证书和第二证书构成的第一证书链发送给第一服务器
S216，第一证书链
S218，基于预设密钥生成算法生成与用户对应的第四公钥
S220，将第四公钥及终端设备的设备信息发给第一服务器
S220，第四公钥及终端设备的设备信息
S222，接收第一服务器发送的目标验证信息和预先构建的证书链
S222，目标验证信息和预先构建的证书链
S224，第一可验证信息
S224，接收第一服务器发送的第一可验证信息
S226，基于第一服务器的第一公钥、终端设备的第二公钥，对证书链中的根证书和第二证书进行验证处理，得到第一验证结果
S228，基于第一服务器的第一公钥和目标验证信息，对第一可验证信息进行验证，得到第二验证结果
S230，基于第一验证结果和第二验证结果，确定验证结果
S232，在验证结果为验证通过的情况下，基于用户的第四私钥，对控车指令进行签名处理，得到第二可验证信息
S234，第三公钥
S234，接收车载设备的第三公钥
S236，，基于车载设备的第三公钥，对控车指令和第二可验证信息进行加密处理，得到加密处理后的控车指令，并将加密处理后的控车指令发送至车载设备
S236，加密处理后的控车指令

图 2A

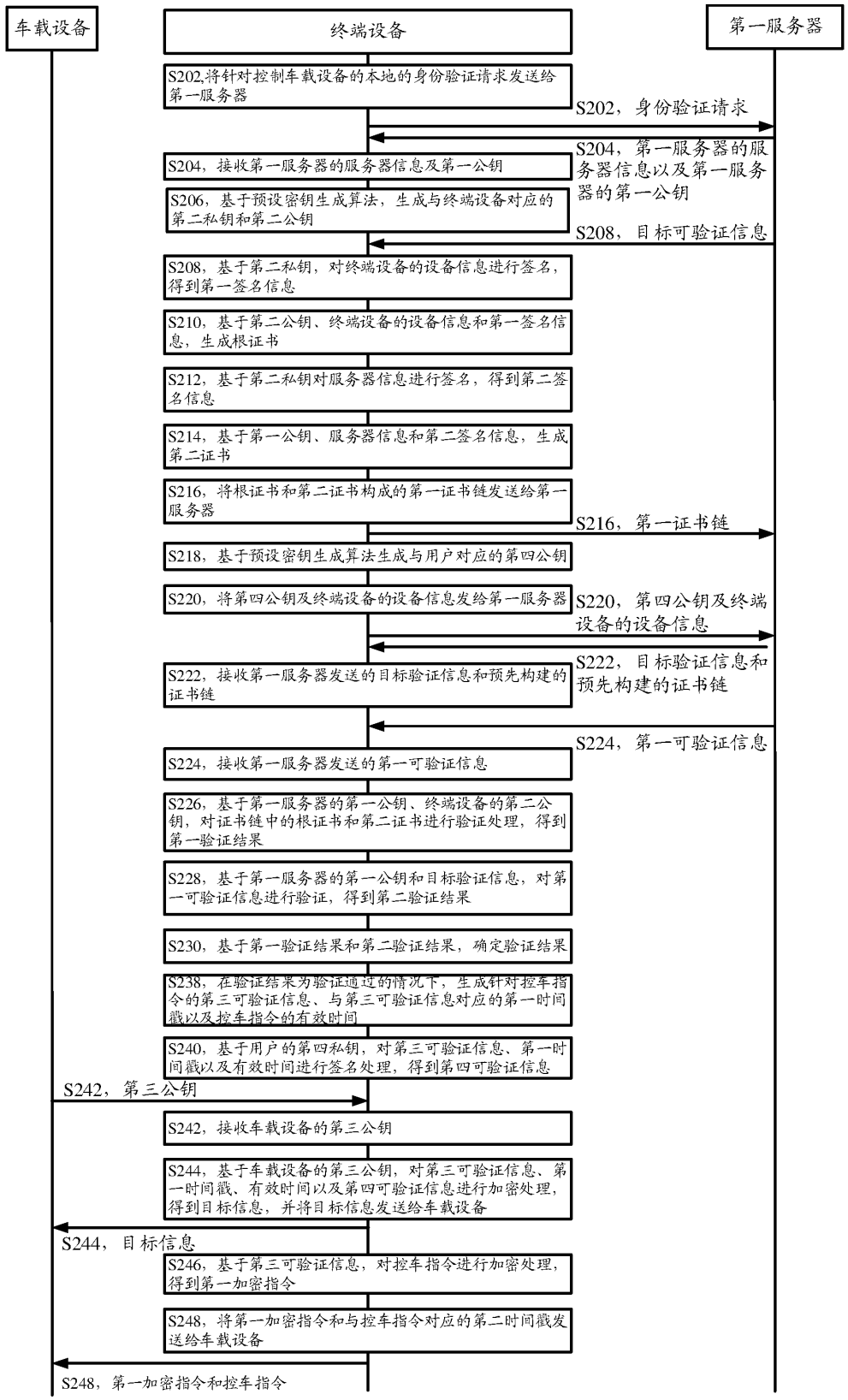

车载设备
终端设备
第一服务器
S202,将针对控制车载设备的本地的身份验证请求发送给第一服务器
S202，身份验证请求
S204，接收第一服务器的服务器信息及第一公钥
S204，第一服务器的服务器信息以及第一服务器的第一公钥
S206，基于预设密钥生成算法，生成与终端设备对应的第二私钥和第二公钥
S208，目标可验证信息
S208，基于第二私钥，对终端设备的设备信息进行签名，得到第一签名信息
S210，基于第二公钥、终端设备的设备信息和第一签名信息，生成根证书
S212，基于第二私钥对服务器信息进行签名，得到第二签名信息
S214，基于第一公钥、服务器信息和第二签名信息，生成第二证书
S216，将根证书和第二证书构成的第一证书链发送给第一服务器
S216，第一证书链
S218，基于预设密钥生成算法生成与用户对应的第四公钥
S220，将第四公钥及终端设备的设备信息发给第一服务器
S220，第四公钥及终端设备的设备信息
S222，接收第一服务器发送的目标验证信息和预先构建的证书链
S222，目标验证信息和预先构建的证书链
S224，第一可验证信息
S224，接收第一服务器发送的第一可验证信息
S226，基于第一服务器的第一公钥、终端设备的第二公钥，对证书链中的根证书和第二证书进行验证处理，得到第一验证结果
S228，基于第一服务器的第一公钥和目标验证信息，对第一可验证信息进行验证，得到第二验证结果
S230，基于第一验证结果和第二验证结果，确定验证结果
S238，在验证结果为验证通过的情况下，生成针对控车指令的第三可验证信息、与第三可验证信息对应的第一时间戳以及控车指令的有效时间
S240，基于用户的第四私钥，对第三可验证信息、第一时间戳以及有效时间进行签名处理，得到第四可验证信息
S242，第三公钥
S242，接收车载设备的第三公钥
S244，基于车载设备的第三公钥，对第三可验证信息、第一时间戳、有效时间以及第四可验证信息进行加密处理，得到目标信息，并将目标信息发送给车载设备
S244，目标信息
S246，基于第三可验证信息，对控车指令进行加密处理，得到第一加密指令
S248，将第一加密指令和与控车指令对应的第二时间戳发送给车载设备
S248，第一加密指令和控车指令

图 2B

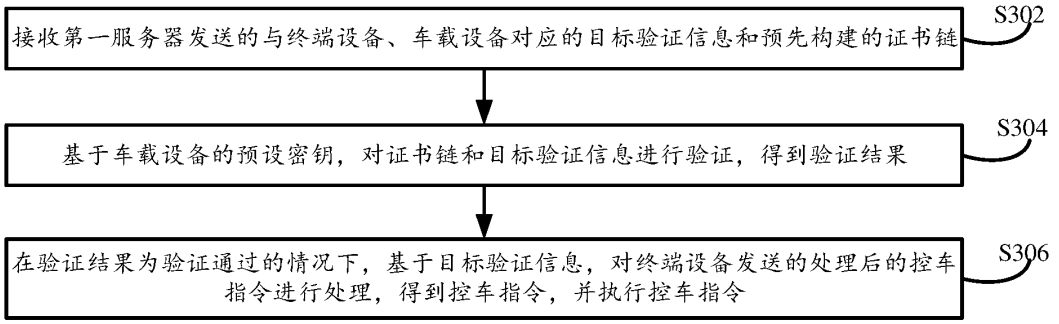

接收第一服务器发送的与终端设备、车载设备对应的目标验证信息和预先构建的证书链
S302
基于车载设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果
S304
在验证结果为验证通过的情况下，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行控车指令
S306

图 3A

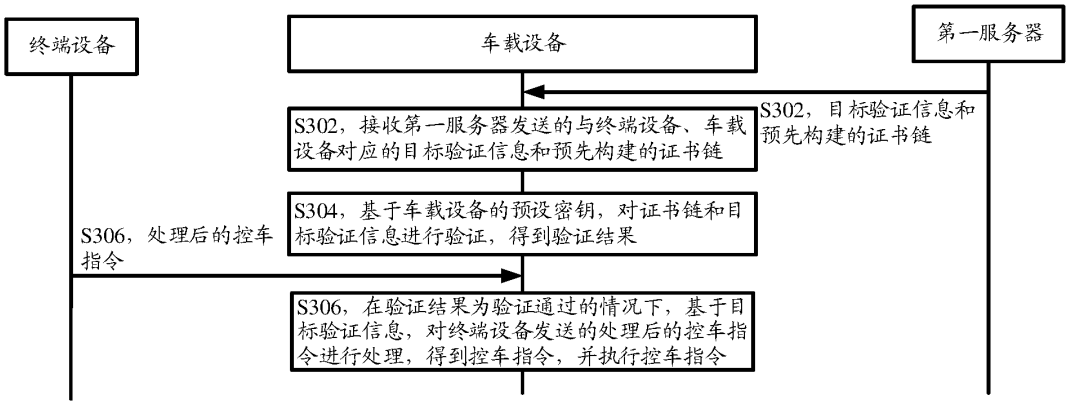

终端设备
车载设备
第一服务器
S302，目标验证信息和预先构建的证书链
S302，接收第一服务器发送的与终端设备、车载设备对应的目标验证信息和预先构建的证书链
S304，基于车载设备的预设密钥，对证书链和目标验证信息进行验证，得到验证结果
S306，处理后的控车指令
S306，在验证结果为验证通过的情况下，基于目标验证信息，对终端设备发送的处理后的控车指令进行处理，得到控车指令，并执行控车指令

图 3B

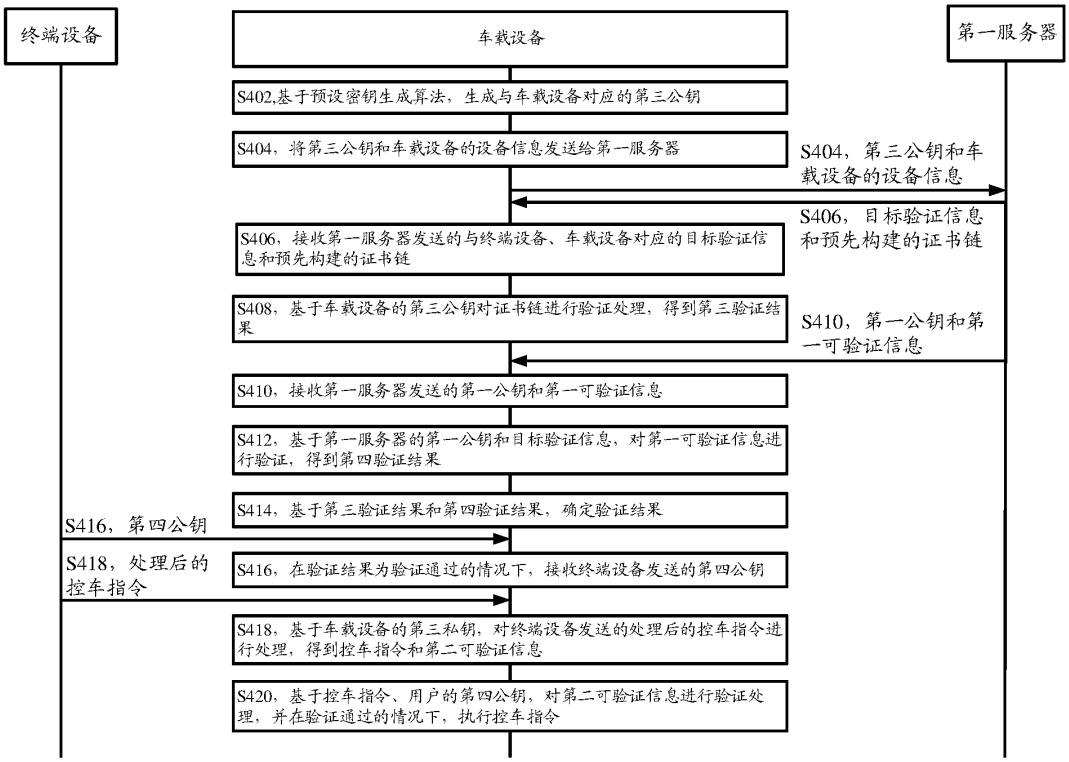

终端设备
车载设备
第一服务器
S402,基于预设密钥生成算法，生成与车载设备对应的第三公钥
S404，将第三公钥和车载设备的设备信息发送给第一服务器
S404，第三公钥和车载设备的设备信息
S406，目标验证信息和预先构建的证书链
S406，接收第一服务器发送的与终端设备、车载设备对应的目标验证信息和预先构建的证书链
S408，基于车载设备的第三公钥对证书链进行验证处理，得到第三验证结果
S410，第一公钥和第一可验证信息
S410，接收第一服务器发送的第一公钥和第一可验证信息
S412，基于第一服务器的第一公钥和目标验证信息，对第一可验证信息进行验证，得到第四验证结果
S414，基于第三验证结果和第四验证结果，确定验证结果
S416，第四公钥
S418，处理后的控车指令
S416，在验证结果为验证通过的情况下，接收终端设备发送的第四公钥
S418，基于车载设备的第三私钥，对终端设备发送的处理后的控车指令进行处理，得到控车指令和第二可验证信息
S420，基于控车指令、用户的第四公钥，对第二可验证信息进行验证处理，并在验证通过的情况下，执行控车指令

图 4A

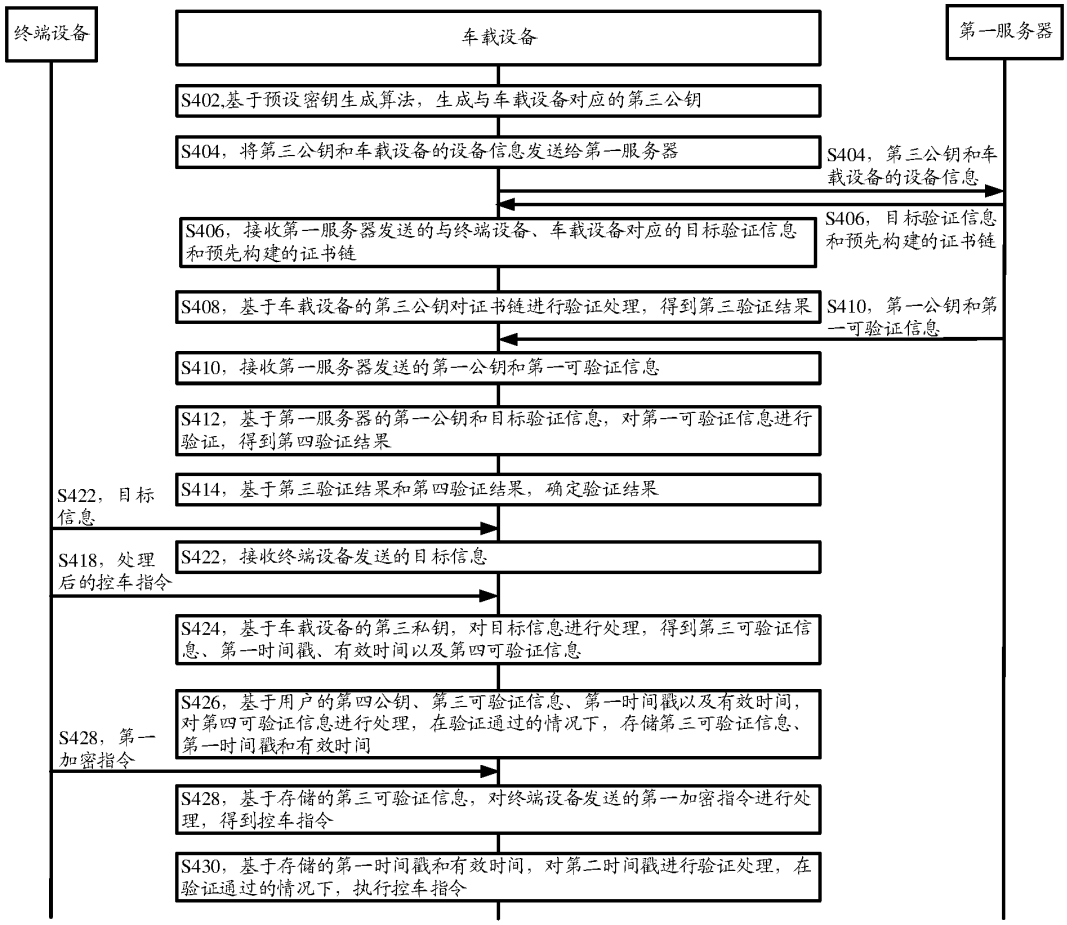

终端设备
车载设备
第一服务器
S402,基于预设密钥生成算法，生成与车载设备对应的第三公钥
S404，将第三公钥和车载设备的设备信息发送给第一服务器
S404，第三公钥和车载设备的设备信息
S406，接收第一服务器发送的与终端设备、车载设备对应的目标验证信息和预先构建的证书链
S406，目标验证信息和预先构建的证书链
S408，基于车载设备的第三公钥对证书链进行验证处理，得到第三验证结果
S410，第一公钥和第一可验证信息
S410，接收第一服务器发送的第一公钥和第一可验证信息
S412，基于第一服务器的第一公钥和目标验证信息，对第一可验证信息进行验证，得到第四验证结果
S414，基于第三验证结果和第四验证结果，确定验证结果
S422，目标信息
S422，接收终端设备发送的目标信息
S418，处理后的控车指令
S424，基于车载设备的第三私钥，对目标信息进行处理，得到第三可验证信息、第一时间戳、有效时间以及第四可验证信息
S426，基于用户的第四公钥、第三可验证信息、第一时间戳以及有效时间，对第四可验证信息进行处理，在验证通过的情况下，存储第三可验证信息、第一时间戳和有效时间
S428，第一加密指令
S428，基于存储的第三可验证信息，对终端设备发送的第一加密指令进行处理，得到控车指令
S430，基于存储的第一时间戳和有效时间，对第二时间戳进行验证处理，在验证通过的情况下，执行控车指令

图 4B

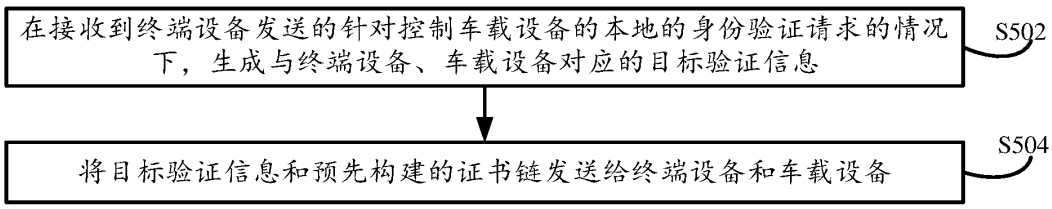

在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与终端设备、车载设备对应的目标验证信息
S502
将目标验证信息和预先构建的证书链发送给终端设备和车载设备
S504

图 5A

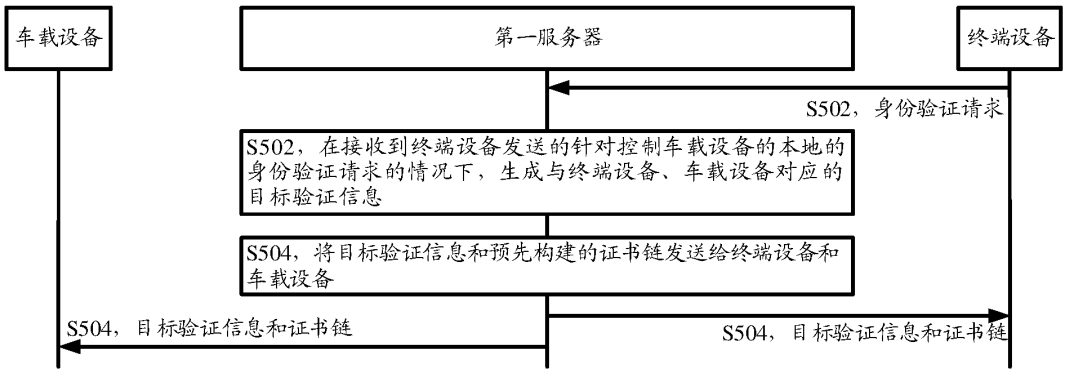

车载设备
第一服务器
终端设备
S502，身份验证请求
S502，在接收到终端设备发送的针对控制车载设备的本地的身份验证请求的情况下，生成与终端设备、车载设备对应的目标验证信息
S504，将目标验证信息和预先构建的证书链发送给终端设备和车载设备
S504，目标验证信息和证书链
S504，目标验证信息和证书链

图 5B

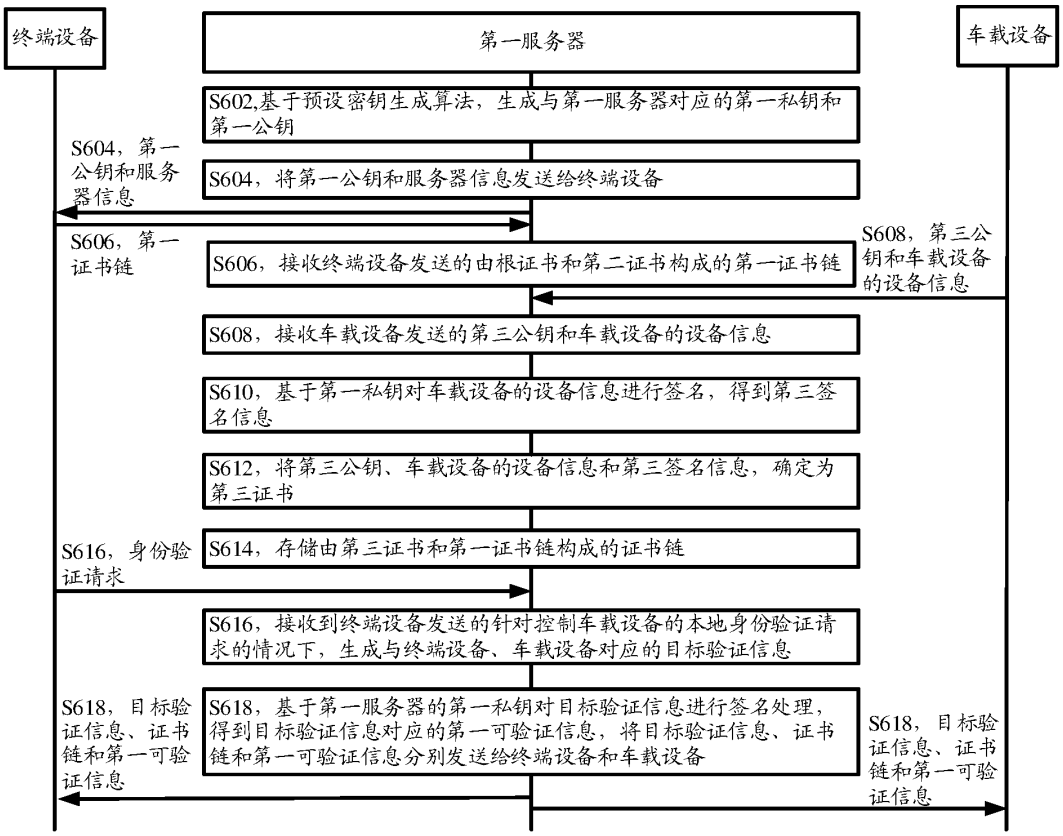

终端设备
第一服务器
车载设备
S602,基于预设密钥生成算法，生成与第一服务器对应的第一私钥和第一公钥
S604，第一公钥和服务器信息
S604，将第一公钥和服务器信息发送给终端设备
S606，第一证书链
S606，接收终端设备发送的由根证书和第二证书构成的第一证书链
S608，第三公钥和车载设备的设备信息
S608，接收车载设备发送的第三公钥和车载设备的设备信息
S610，基于第一私钥对车载设备的设备信息进行签名，得到第三签名信息
S612，将第三公钥、车载设备的设备信息和第三签名信息，确定为第三证书
S614，存储由第三证书和第一证书链构成的证书链
S616，身份验证请求
S616，接收到终端设备发送的针对控制车载设备的本地身份验证请求的情况下，生成与终端设备、车载设备对应的目标验证信息
S618，目标验证信息、证书链和第一可验证信息
S618，基于第一服务器的第一私钥对目标验证信息进行签名处理，得到目标验证信息对应的第一可验证信息，将目标验证信息、证书链和第一可验证信息分别发送给终端设备和车载设备
S618，目标验证信息、证书链和第一可验证信息

图 6

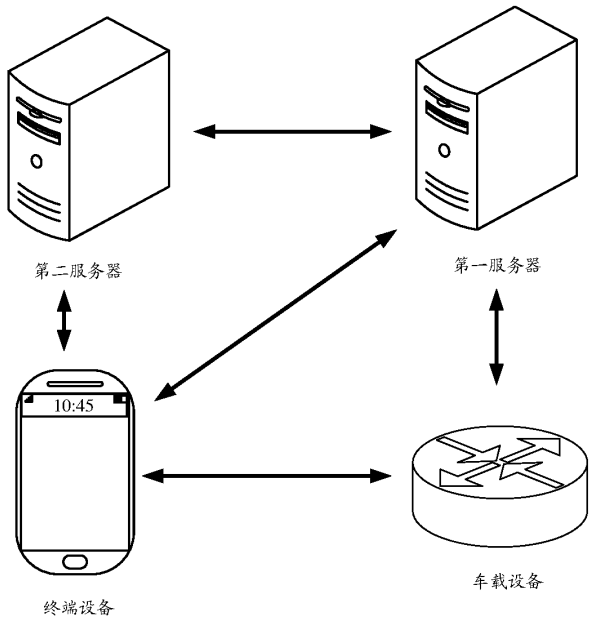

第二服务器
第一服务器
10:45
终端设备
车载设备

图 7

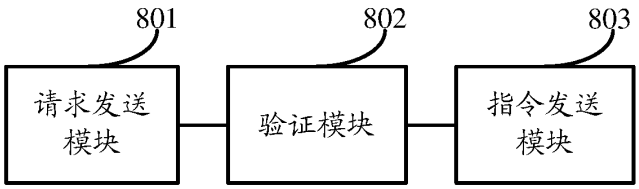

801
802
803
请求发送模块
验证模块
指令发送模块

图 8

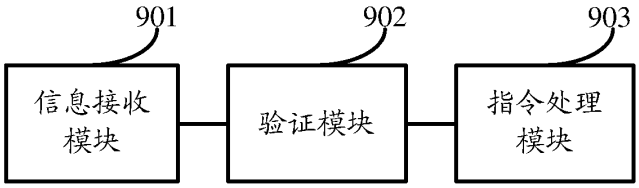

901
902
903
信息接收模块
验证模块
指令处理模块

图 9

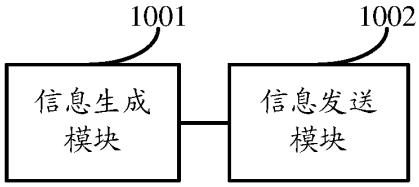

1001
1002
信息生成模块
信息发送模块

图 10

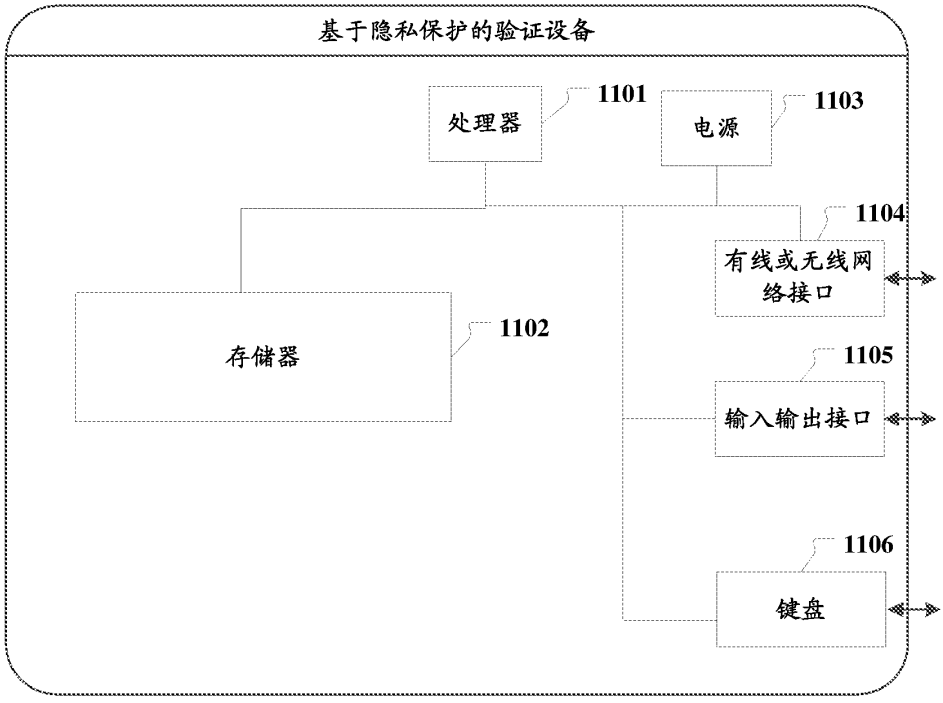

基于隐私保护的验证设备
处理器
1101
电源
1103
1104
有线或无线网络接口
存储器
1102
1105
输入输出接口
1106
键盘

图 11