Unified Script File Format for Provisioning the ADF in a FiRa Applet

Steven Liu (steveliu@google.com)
Ning Zhang (zning@google.com)

ABSTRACT

[0001] The Common Service Management Layer (CSML) section of the FiRa specification defines certain procedures that facilitate communicating with a secure element of a device to further facilitate the generation of a dynamic scrambled timestamp sequence (STS). Some of these procedures involve communicating an application protocol data unit (APDU) script file from a service provider to a UWB-enabled device and, in particular, to a FiRa applet operating on the device. The specification does not define a standard format for the script file.

[0002] This shortcoming is addressed herein by specifying a standard format for the script file in the FiRa specification (e.g., in the Common Service Management Layer (CSML) section of the FiRa specification.

INTRODUCTION

[0003] Some devices are equipped with ultra-wideband (UWB) circuitry that facilitates communicating information with other similarly equipped devices. The UWB modulation techniques used by these devices facilitate determining the distance between devices to within centimeters. UWB tends to work well in environments where multipath interference is exhibited (e.g., indoor environments), and circuitry that implements UWB requires a relatively low amount of power.

[0004] Various standards have been proposed to standardize UWB communications between devices. One such standard is promulgated by the FiRa consortium. The FiRa standard specifies several different packet configurations for communicating information between FiRa-compliant devices. This, in turn, facilitates determining the distance between the devices.

[0005] The FiRa standard specifies various encryption techniques to apply to UWB packets to secure UWB communications between compliant devices. One encryption technique involves encrypting information in the packet based on a predefined/static session key, the value of which is specified in the standard. Another technique involves encrypting information in the packet based on a dynamic session key that is derived from a secure element of one of the devices. The secure element corresponds to a dedicated processor that performs cryptographic operations without revealing decrypted information on a computer bus. The STS referred to above may be encrypted based on the dynamic session key. For example, Advanced Encryption Standard 128 (AES-128) logic may be used to encrypt the STS using the dynamic session key to derive an encrypted/dynamic STS.

[0006] The Common Service Management Layer (CSML) section of the FiRa specification defines certain procedures that facilitate communicating with the secure element to support generating a dynamic STS. Referring to Figure 1, these procedures involve communicating an application protocol data unit (APDU) script file from a service provider to a UWB-enabled device and, in particular, to a FiRa applet operating on the device. The APDU script file comprises one or more APDUs associated with one or more types of secure element that may be operating on a device. Each APDU defines the fundamental data structure and format for communicating information to and from a corresponding secure element. (*See* ISO7816-4) The APDU script file may further specify procedures in the form of instruction code that the FiRa applet should follow when communicating with the secure element.

[0007] The FiRa applet may, in turn, communicate the APDU script file to a framework proxy of the device. The framework proxy (or FiRa applet) may then parse and execute the APDU script file and configure the application dedicated file (ADF) of the FiRa applet to facilitate UWB

communications. (The ADF corresponds to data structure within the application data structure that hosts, for example, applications and application specific data as described in ISO/IEC 7816-4). For example, the framework proxy (or the FiRa applet) may communicate with the secure element according to the APDUs and instructions in the script file to assist session key derivation and exchange.

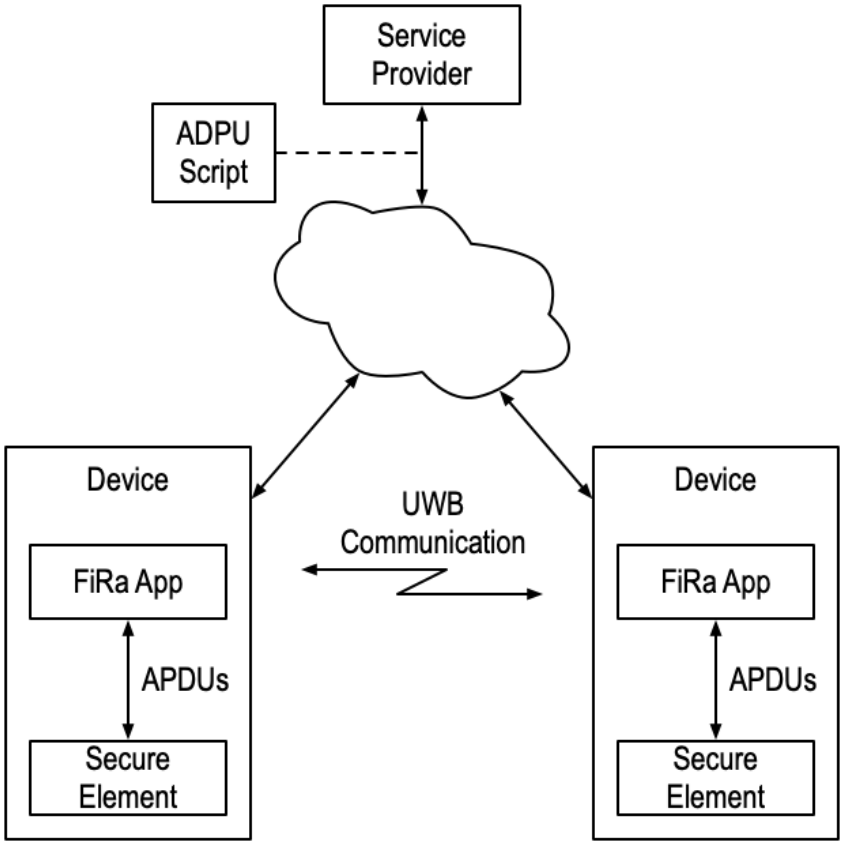

Figure 1
(APDU Script Communication)

[0008] The CSML standard does not, however, specify a standard format for the APDU script file. Therefore, 3rd party FiRa applets (e.g., applets not affiliated with the service provider) may be unable to parse the APDU script file.

[0009] This shortcoming can be addressed by specifying a standard format for the script file in the FiRa specification (e.g., in the CSML section of the FiRa specification). A service provider

that complies with the standard may communicate the script file using the specified format. In some examples of the standard format, the above-referenced ADPUs and/or procedures are specified in JavaScript Object Notation (JSON), Concise Binary Object Representation (CBOR), a UTF-8 encoded text file, XML, etc. In some examples of the standard format, a Multipurpose Internet Mail Extension (MIME) or content-type header that specifies the particular format of the ADPU script file is included at the beginning of the script file. In some examples of the standard format, the ADPUs are specified as a string of hexadecimal digits, base 10 digits, octal digits, etc., delimited by a comma, tab, line break, etc.

[00010] Some examples of the standard can further require the communication of a digital signature that facilitates authentication of the script file. For example, a service provider that complies with this aspect may generate a cyclic redundancy check (CRC) code associated with the script file and communicate the CRC code to the FiRa applet. Some examples of the digital signature are generated by a trusted authority and facilitate confirming the integrity and authenticity of the FiRa applet. Some examples of the standard can require the script file to be encrypted. For example, the FiRa applet operating on a particular device may communicate a public encryption key to the service provider, which the service provider may use to encrypt script files destined for the device.