|  |  |
| --- | --- |
| 1 | M. Roland and J. Langer, "Digital Signature Records for the NFC Data Exchange Format," 2010 Second International Workshop on Near Field Communication, Monaco, 2010, pp. 71-76.  doi: 10.1109/NFC.2010.10  Abstract: The NFC Data Exchange Format (NDEF) is a standardized format for storing formatted data on NFC (Near Field Communication) tags and for transporting data across a peer-to-peer NFC link. Through NDEF and its various record types, events can be triggered on an NFC device by simply touching an NFC-enabled object. The number of use cases and real applications around NFC and NDEF technology increases continuously. However, existing applications provide hardly any protection against (malicious) manipulation of NDEF data. Digital signatures are a means of providing authenticity and integrity of NDEF data. Therefore, the NFC Forum - which is responsible for the specification of data formats, protocols and applications in regard to the NFC technology - is working on adding digital signatures to their NDEF format. While their signature record type is still in draft status and has not been released to the public, this paper discusses the various aspects of digitally signing NDEF records. First, we introduce the readers to the NFC Data Exchange Format, its use cases and its potential security threats. After that, we describe the potential of digital signatures for NDEF messages. Finally, we discuss the advantages and disadvantages of various ways to digitally sign an NDEF message.  keywords: {digital signatures;electronic data interchange;NDEF data authenticity;NFC data exchange format;digital signature records;digitally signing NDEF records;formatted data storing;near field communication;potential security threats;Communications technology;Digital signatures;Emulation;IEC standards;ISO standards;Internet telephony;Peer to peer computing;Protocols;Radiofrequency identification;Transponders;Digital signature;NFC Data Exchange Format (NDEF);Near Field Communication (NFC);Record Type Definition (RTD);Security},  URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5476460&isnumber=5476454 |
|  |  |
|  |  |
|  |  |
|  |  |