

في حال الرغبة بتأمين الحامل الإلكتروني من قبل الزبون/الجهة، يجب أن يحقق الحامل الإلكتروني المواصفات التالية كحد أدنى:

- يدعم الخوارزمات RSA و/أو ECDSA
- طول المفتاح الذي يمكن توليده ضمن الحامل لا يقل عن 2048 بالنسبة لخوارزمية RSA ولا يقل عن 256 بالنسبة لخوارزمية ECDSA
- يمكن توليد المفاتيح الخاصة ضمن الحامل الإلكتروني
- تدعى إمكانية منع تنصير المفتاح الخاص لخارج الحامل الإلكتروني
- تدعى إجراء عمليات التوقيع والتشفير وفك التشفير داخل الحامل الإلكتروني



From: /https://info.ecc.sy - مركز معلومات مركز التصديق

Permanent link:
https://info.ecc.sy/doku.php?id=docs:token_spec

Last update: 2024/01/30 07:31