1. **Интерен Акт за информатичко поврзување, поврзување за пренос на податоци и безбедносни стандарди**

Од аспект на безбедност, информатичко поврзување за пренос на податоци подразбира различни типови на безбедносен пристап од страна на сите учесници во комуникациските системи, односно учесниците на пазарот.

Безбедносните стандарди се применуваат за да се овозможи проверка на автентичноста на потписникот, заштита на интегритетот на податоците кои се пренесуваат и неотповикливост на електронскиот потпис на датата на пораката или документот.

Секој од учесниците на пазарот треба да поседува дигитален сертификат за веродостојноста на неговиот идентитет.

Се дефинираат два режими на работа: стандарден режим и backup режим.

- **Стандарден режим:** За да учесникот на пазарот пристапи на системите на ОЕПС и ОПЕЕ треба да располага барем со еден од наведните начини, во зависност од апликацијата/софтверот кој се употребува:
  - https пристап
  - PKI (Public Key Infrastructure) token - клуч со електронски сертификат
  - E-mail (корпорациски е-маил) со дигитален потпис
  - Корисничко име (User name) и лозинка (Password)

- **Backup режим:** Backup режимот се применува во ситуации настанати од непланирани нерасположивости на системите ОЕПС и ОПЕЕ, а во сите други случаи важи стандардната процедурата, односно стандардниот режим на работа. За да учесникот на пазарот пристапи на системите на ОЕПС и ОПЕЕ треба да располага барем со:

- Факс (со претходно договорени/дефинирани телефонски броеви)
- Телефон

Доколку дојде до нерасположивост на системите ОЕПС и ОПЕЕ, учесниците на пазарот ќе бидат известени за премин во Backup режим на работа како и за сите дополнителни промени, преку е-маил, факс и сл.