

Електронні ключі SecureToken-338 —апаратно-програмні пристрої, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки. Відповідно до Закону України «Про електронні довірчі послуги» є засобами кваліфікованого електронного підпису чи печатки.



Призначені для використання в системі електронних довірчих послуг України.

SecureToken-338 мають позитивні експертні висновки Державної служби спеціального зв'язку та захисту інформації України № 04/03/02-2160 від 18.08.2020 і № 04/03/02-133 від 20.01.2020.

SecureToken-338 реалізують криптографічні алгоритми електронного підпису, визначені законодавством України:

- ДСТУ 4145-2002 з довжиною ключа 163-509 біт;
- RSA з довжиною ключа 1024-4096 біт;
- ECDSA з довжиною ключа 192-521 біт;
- обчислення геш-функцій відповідно до ДСТУ 7564-214, SHA-1, SHA-512, ГОСТ 34.311-95.

Працюють у комп'ютерних системах під управлінням Windows XP/Vista/7/8/10, Windows Server 2003/2012/2016, Linux, Mac OS, Linux, Android.

Мають відкриті прикладні інтерфейси (API): PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, MS minidriver, CNG.

Електронні ключі **SecureToken-338** виготовляються в Україні відповідно до ТУ У 26.2-32248356-029:2020 у трьох модифікаціях, які відрізняються лише зовнішнім виглядом і типом корпусу:

1. SecureToken-338S (АЧСА.467369.043) – металевий корпус із сплаву цинку та алюмінію.
2. SecureToken-338M (АЧСА.467369.033) – пластиковий малогабаритний корпус із полівінілхлорида.

Усі модифікації SecureToken-338 є повністю сумісними.

Електронні ключі мають надійну вбудовану систему захисту від зчитування інформації та її підробки та відповідають високому рівню захищеності по європейським критеріям. Смарт-чипи сімейства SLE78CxFXxxxxP компанії Infineon Technologies AG (Німеччина), які використовуються у пристроях, відповідають міжнародному рівню безпеки Common Criteria EAL6+.

Захист від підбору паролю: знищення особистого ключа після 7 невдалих спроб підбору підряд.

Термін служби становить 10 років. Гарантія 12 місяців.