

# Protiva™ Smart Guardian

||||| En högre säkerhetsnivå för känslig data



## FÖRETAG > PRODUKT

En av de största utmaningarna i fråga om informationssäkerhet idag är att skydda de stora mängder av personliga och konfidentiella data som används av företag och myndigheter. USB-minnen är ett speciellt problem, eftersom många anställda använder dem för att lagra känslig information och de lätt kan tappas bort eller stjälas. Om ett företag förlorar sin information, kan den ekonomiska följden vara enorm och därför måste någonting göras. Många företag utvecklar nu mer anpassade lösningar för att minska risken för dataförlust, bl.a. genom kryptering av data och ytterst noggrann kontroll av USB-minnen.

En egenskap av ledare inom digital säkerhet erbjuder Gemalto användarna mycket säkra enheter som ger enskild åtkomst till nätverk, applikationer och data. Dess säkra USB-tokens skyddar data som lagrats offline genom att kontrollera åtkomsten till enhetens flashminne och kryptera data som lagrats i det. De lösningar som Gemalto erbjuder för att förebygga dataförluster är enkla att använda och kan integreras i företagets policy för USB-minnen för att uppnå den högsta säkerhetsnivån för flyttbara data.

### Protiva™ Smart Guardian: enkel att använda

Smart Guardian är en personlig

### > Viktiga egenskaper

- Enkel plug-and-play-användning och kompatibel med de flesta operativsystem
- Fungerar med marknadstillgängliga produkter för kontroll av slutpunkter
- Stöder PKCS#11-baserad smartkortsfunktion och autentisering av engångslösenord
- Uppfyller kraven för certifieringen FIPS 140-2 nivå 3
- Tillgänglig med minneskapacitet på 2 eller 4 GB

säkerhetsenhet som skyddar flyttbara data med Gemaltos beprövade smartkortsteknik. Till skillnad från andra säkra USB-minnen, ger den en oöverträffad nivå av dataskydd, eftersom alla känsliga funktioner och kryptografiska nycklar styrs internt från smartkortets säkra miljö.

Användarna sticker bara in Smart Guardian i en USB-port och autentiserar sig med ett lösenord. Lösenordet godkänns av smartkortet som låser upp enheten, varefter känsliga filer kan överföras, kopieras

eller lagras på den säkra volymen och sedan krypteras. Om flera felaktiga lösenord matas in över ett förutbestämt antal gånger i följd, låses enheten för att skydda sina data mot attacker och otillåten åtkomst till krypteringsnycklarna. Enheten kan då låsas upp av en administratör antingen lokalt eller fjärrstyrt med en PKI-baserad metod (öppen nyckelteknik). Efter kopieringen kan Smart Guardian låsas och tas ut med säkerhet genom att välja det lämpliga kommandot i den kontextuella menyn.

Smart Guardian erbjuder en komplett, personaliserad datasäkerhet, som är lätt för IT-administratörer att utnyttja och hantera. Den stöder många operativsystem och kräver inga styrprogram vilket betyder att den är snabb och effektiv att ta i drift. Smart Guardian stöds av Token Lifecycle Manager, en omfattande portal för hantering av tokens. Gemalto står bakom denna portal som ger användare och administratörer möjlighet att registrera nya enheter, uppdatera mjukvaran i enheterna, ändra registreringsuppgifter, samt låsa och låsa upp tokens.

# Protiva™ Smart Guardian

IIIIII Personaliserat skydd för känsliga data

## ■ Viktiga fördelar

### > Högsta skyddsnivån för USB-data genom smartkortsteknik

Inne i Smart Guardian finns ett smartkort som gör enheten manipulerings säker, detta smartkort är en högpresterande mikroprocessor som genererar kryptografiska nycklar som används för att kryptera och dekryptera data. Det är alltså omöjligt att komma åt krypteringsnyckeln, eftersom den skyddas av smartkortet.

Eftersom Smart Guardian baserar sig på smartkortsteknik erbjuder den en mycket högre säkerhetsnivå än PIN-skyddade USB-minnen som är relativt vanliga men långt ifrån lika säkra. Säkerhetsfunktionerna i smartkortets modul och den integrerade programvarans säkra uppbyggnad hjälper till att skydda mot hårdvaru- och mjukvarubaserade angrepp.

### > Förstärka säkerhetspolicyn för flyttbara data

Smart Guardian fungerar tillsammans med andra leverantörer av säkerhetsprodukter för att skapa en komplett lösning för att förebygga dataförluster. Den möjliggör en ytterst anpassad kontroll av data som lagrats och är åtkomliga via USB-minnen i företagets hela nätverk.

### > Lägre inköpskostnad i jämförelse med andra lösningar

Genom att Smart Guardian uppfyller industristandarder, är kompatibel med många operativsystem och har en PKCS#11-baserad smartkortsteknik, erbjuder den betydande kostnadsfördelar för företag som behöver utveckla lösningar för sina flyttbara data.



### > Enkel anpassning till existerande infrastruktur

Smart Guardian har ett standard USB-gränssnitt och fungerar på Windows och Mac operativsystem, så enheten är ytterst anpassningsbar. Tillsammans med portalen Token Lifecycle Manager som Gemalto står bakom erbjuder den en komplett lösning som lätt kan integreras i existerande IT-infrastrukturer.

### > Flexibelt stöd till ett stort antal säkerhetsapplikationer

PKCS#11 stödet erbjuder flexibilitet att integrera andra applikationer i Smart Guardian-enheten, som t.ex. digital signatur, säker fjärråtkomst, autentisering med engångslösenord och andra PKI-baserade tjänster.

## > Smartkortstekniken förstärker datasäkerheten

Smartkortstekniken erbjuder flera fördelar för säkra datalagringsenheter:

### Flyttbarhet och lätthanterlighet

Digitala certifikat och krypteringsnycklar lagras alltid på kortet, inte externt. Denna enhet som fungerar med smartkortsteknik kan användas från alla system utan att ge vika på säkerheten.

### Säker åtkomst

Endast den auktoriserade användaren har åtkomst till sina data med hjälp av 2-faktors autentisering via smartkortets operativsystem.

### Kryptografi

Smarta kort omfattar en bred serie kryptografiska möjligheter, inklusive generering av nycklar, säker nyckelförvaring, dataspridning (hashing) osv., som används för att skydda data som lagrats i flashminnet.



[www.gemalto.com](http://www.gemalto.com)

**gemalto**  
security to be free