GTP – GENERELL TEKNISK PLATTFORM - för informations- och ledningssystem

GTP – Generell Teknisk Plattform – en säkerhetsprodukt med samverkande säkerhetskomponenter. Med GTP fås en teknisk IT-infrastruktur som ger en säker driftsmiljö för nätverks- och tjänstebaserade tillämpningar.

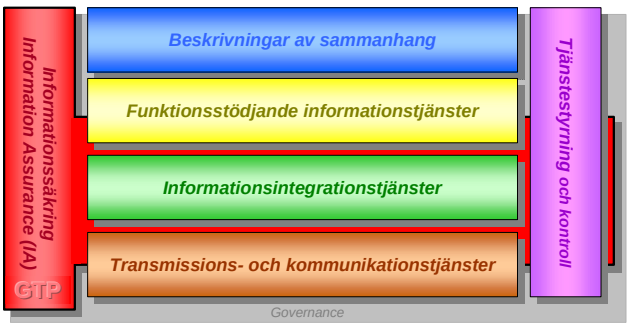
GTP består av ett antal programvaruprodukter som levereras i form av CD/DVD media. För att snabbt komma igång, finns även en GTP säkerhetsserver att koppla in på nätet.

GTP innehåller säkerhetskomponenter för att uppfylla krav på sekretess, integritet, tillgänglighet och spårbarhet i verksamhetsfunktioner för alla slags informations- och ledningssystem.

Med GTP kan utvecklingsresurserna koncentreras på verksamhetsfunktioner snarare än säkerhetsfunktioner. GTP tillhandahåller säkerhetskomponenter som redan passar ihop som prefabricerade pusselbitar, färdiga att kopplas in, för att uppfylla systemens olika säkerhetskrav.

Säkerhetskrav har beroenden sinsemellan vilket innebär att säkerhetskomponenterna behöver passa ihop samt kunna samverka säkert via en ”säkerhetsbuss”. Exempelvis kräver en hållbar loggning en tillförlitlig identifiering av användaren. För att uppnå hög assurans är säkerhetskomponenterna och säkerhetsbussen i GTP utformade enligt en modern operativsystemoberoende säkerhetsarkitektur (IRMA, Independent Reference Monitor Architecture).

GTPs säkerhetskomponenter, passar väl in i olika strukturer för beskrivning av informationssäkring såsom NISP IA (Information Assurance) och FMLS TS designmönster.



GTP fungerar för såväl befintliga som nya system.

GTP ger säkerhet för färdigutvecklade samt kommersiella tillämpningar, så kallade COTS, utan att dessa behöver ändras eller anpassas. GTP lämpar sig även för egenutvecklade tillämpningar byggda med tjänsteorienterad eller med annan teknik. Även för dessa fås ökad säkerhet utan att tillämpningarna behöver modifieras. I GTP finns också gränssnitt (APIer) för utvecklare som själv önskar anropa säkerhetstjänster.

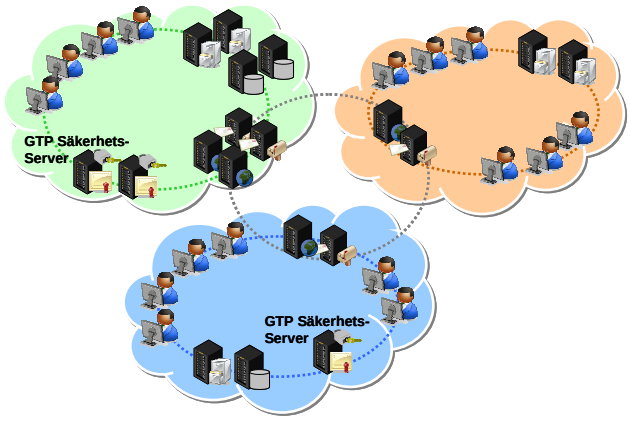
GTP är flexibel och kan användas i olika systemmiljöer såsom Microsoft Windows samt olika slags UNIX. GTP kan användas både på traditionella ”tjocka” klienter och ”tunna” lösningar för fjärruppkoppling mot Citrix och Windows Terminal Server. GTP kan också användas i webb och SOA-baserade lösningar.

GTP är resurseffektivt och har god skalbarhet, från några få till tusentals nätverksanvändare. GTPs tjänster är dynamiska och hittar själv varandra i nätet.

Färdig att använda

GTP är en beprövad standardprodukt som inte kräver anpassning av befintlig programvara, datorer eller nätverk. Med GTP undviks stora investeringar i att behöva bygga om och anpassa befintliga system för att erhålla ökad säkerhet.

GTP införs genom att en eller flera säkerhetsservrar (maskinvara) kopplas in på nätet. Därefter installeras de säkerhetskomponenter (programvara) som önskas på övriga datorer i nätet. Efter konfigurering kan samtliga tillämpningar få nytta av de flesta funktioner i GTP.



GTP tillför också gemensamma administrations- och övervakningsfunktioner i nätet. GTP ger därmed möjlighet till en sammanhållen administrations- och säkerhetslösning för flera samverkande system i blandade (Windows, UNIX) systemmiljöer.

Säker informationshantering

För att tillgodose höga säkerhetskrav enligt sekretesslagen, MUST KSF, EU och NATO krav m.fl., finns i GTP ett antal säkerhetskomponenter. De innefattar Single Sign-On (SSO) med olika metoder för identifiering, bl.a. aktiva kort (inom Försvarsmakten - TAK2 och TEID), bankers elektroniska ID, mjuka certifikat och lösenord. Vidare komponenter för åtkomstkontroll, loggning, integritets-

kontroll, skydd mot skadlig kod, säker styrning och övervakning m.m.

Inloggningsfunktionen använder en metakatalog för användare i blandade systemmiljöer (s.k. ”Identity Management”). Efter godkänd inloggning i GTP och nätet blir användaren inloggad i respektive operativsystem. Även tjänster och noder identifieras och loggas in med GTP.

GTP innehåller totalt ett 70-tal konfigurerbara programvarukomponenter. Många av dessa komponenter är COTS som har säkerhetskonfigurerats och satts samman i automatiserade installationspaket. Det finns färdiga paket för olika typer av system och kravnivåer. Arkitekturen i GTP är ”pluggbar” och har stöd för olika säkerhetsmekanismer (kryptoalgoritmer, aktiva kort etc.).

• Behörighetskontroll	✓
▪ Inloggning	✓
▪ Autentisering	✓
▪ Åtkomstkontroll	✓
• Säkerhetsloggning	✓
• Skydd mot obehörig avlyssning	✓ RÖS, KRY utrustning mm kan behövas
• Intrångsskydd	✓ Brandvägg mm förutsätts för extern komm.
• Intrångsdetektering	✓ Regler förutsätts vara definierade
• Skydd mot skadlig kod	✓
• Funktioner för tillgänglighet	✓
• Funktioner för riktighet (Integritet)	✓
• Stark Autentisering (TAK2)	✓
• Förstärkt inloggning (TEID)	✓

GTP är kryptoverifierad och säkerhetsgranskad mot MUST krav på säkerhetsfunktioner (KSF) och är lämplig att använda i system med sekretessklass från Restricted (H/R) till och med Top Secret (H/TS). Tekniskt ackrediteringsunderlag (TAU) för GTP finns för att användas vid ackreditering av system som nyttjar GTP komponenter.

Enkel att använda

Användaren behöver bara göra en inloggning under sitt arbetspass, så kallad Single Sign-On, och får därmed tillgång till de tillämpningar som han/hon behöver. GTP ger också säkerhet i användarfunktioner såsom e-post, samarbetsprogramvara, webb, fjärråtkomst och fildelning. GTP stöder mobilitet och kan ge samma miljö och tillgänglighet oavsett från vilken arbetsplats (klient) inloggningen sker.

Säkerhetsadministratören får ett enkelt och enhetligt verktyg för säkerhetsadministration, övervakning och styrning.

Systemintegratörer nyttjar beprövade verktyg och dokumentation som tidigare använts vid ett flertal systemintegrationer och driftsättningar. Systemutvecklare kan fokusera på framtagning av verksamhetsfunktion.

Effektiv systemförsörjning

GTPs fokus är att lösa vanliga och återkommande säkerhetsproblem i informations- och ledningssystem.

Med GTP går det att anskaffa färdigutvecklade och beprövade system utan att hindras av att dessas nuvarande säkerhetslösningar inte uppfyller svenska säkerhetskrav.

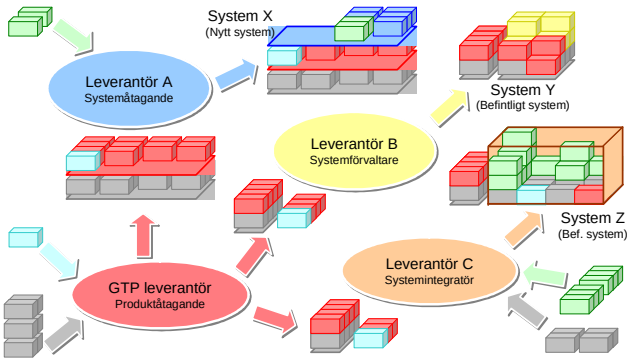
Den totala kostnaden för anskaffning och underhåll minskar genom att flera system kan använda redan verifierade och samverkande säkerhetskomponenter ur GTP.

Risker såväl som kalendertid till driftsatt system reduceras både för upphandlare och leverantör, genom att säkerhetslösningen redan är granskad mot höga säkerhetskrav. Det normalt omfattande arbetet med verifiering och granskning av systemets säkerhetslösning reduceras till att verifiera att GTPs säkerhetsfunktioner nyttjats på föreskrivet sätt enligt checklista.

Upphandling av system blir betydligt enklare och kräver mindre. Genom att kunna referera till en redan existerande säkerhetslösning vid upphandling fås större valfrihet och konkurrens avseende leverantörer av både tillämpningar och system.

En gemensam säkerhetsgrund såsom GTP utgör förutsättning för säker samverkan. Då finns förutsättning för samverkan mellan olika användare och system på ett säkert sätt.

För att underlätta användning av GTP finns dokumentation, utbildning och support samt en beprövad process för införande i olika typer av system.



Funktioner i GTP

- single sign-on (SSO) med aktiva kort (TAK/TEID) – PKI
- autentisering av program, tjänster, datorer
- ömsesidig autentisering
- sessionsskydd, nyckeldistribution och kryptering
- delegering av behörigheter
- åtkomstkontroll nära resurser/information
- säkerhetsloggning
- insamling och skydd av loggar
- logganalys (automatisk och manuell)
- integritetskontroll
- enhetlig administration, metakatalog
- övervakning och styrning
- gemensam meddelandekonsol
- säker programstart
- skydd mot skadlig kod
- säker terminalfunktion (telnet, Citrix och Windows Terminal Services)
- säker mail, webb, filsystem, säkert profillager
- säkerhetskonfiguration av systemmiljöer

För teknisk information kontakta:
Jaan Haabma, Basesoft, 0708-502973
jaan.haabma@basesoft.se
P-O Risberg, Logica, 0733-981558
per.ola.risberg@logica.com

Basesoft

logica be brilliant together