Flödesbeskrivning för uppkoppling av en dator i ett skyddat trådlöst nätverk:

1. Datorn letar efter ett trådlöst nätverk, antingen genom att söka på alla nätverk som annonseras ut i omgivningen och visa dessa i en lista eller genom att användaren på förhand angivit SSID (namnet på aktuellt nätverk), så att datorn kan ansluta direkt mot detta nätverk.
2. Datorn autentiserar sig mot accesspunkten (basstationen) via WPA/802.11x eller WPA-PSK. Autentisering innebär att datorn blir identifierad och godkänd av accesspunkten för vidare uppkoppling och kommunikation.
3. Direkt efter avklarad autentisering påbörjas dataöverföringen och den krypteras (skyddas) med valt krypteringsprotokoll (TKIP eller AES). Protokollet innehåller förutom själva krypteringsalgoritmen (RC4 för TKIP och Rijndael för AES) även hantering av automatisk skapande av ny nyckel för varje enskilt paket som skickas m.m.

Ordlista och tips för finjustering av säkerheten:

Kryptering = Process för att göra läslig information (klartext) oläslig genom ett chiffer. Motsatsen, d.v.s. göra oläslig information läslig igen kallas **dekryptering**.

Chiffer = En algoritm för att genomföra en kryptering.

Nyckel = Kan enkelt förklaras som den information som krävs för att dekryptera ett chiffer, d.v.s. göra oläslig text läslig igen. Kallas även lösenord, passphrase, pre-shared key m.m.

WEP = Standard för autentisering och kryptering. Kryptering av dataöverföringen sker med WEP och RC4 strömchiffer. WEP har inget sätt att dynamiskt byta sina nycklar, vilket är negativt då samma nyckel används om och om igen i alla paket som skickas fram och tillbaka. På det sättet kan man med efter en kort tids informationsinsamling knäcka nyckeln. Detta är ett osäkert protokoll och bör undvikas i möjligaste mån!

Öppen nyckelautentisering (WEP) = Används öppen nyckel skickar datorn och basstationen krypterad data direkt och dekryptering sker med samma statiska nycklar.

Delad nyckelautentisering (WEP) = Används delad nyckel skickar basstationen en så kallad klartextsutmaning (challenge text) till datorn, som i sin tur krypterar den med sin nyckel och skickar tillbaka den till basstationen.Basstationen kontrollerar svaret genom att själv kryptera klartextutmaningen och jämföra det med det mottagna svaret och blir resultatet samma vet basstationen att det är samma nyckel som använts och därmed är autentiseringen genomförd. Detta sätt innehåller svagheter, eftersom man kan räkna ut nyckeln genom att tillräckligt många paket samlas in.

WPA = Standard för autentisering och kryptering. Autentisering sker med 802.11x/EAP mot en autentiseringsserver. Kryptering av dataöverföringen sker med ett av två olika protokoll (TKIP och AES).

WPA-PSK = Samma som WPA, men med på förhand delad statisk nyckel (lösenord) för autentiseringen. Samma nyckel anges i accesspunkten och i datorn. Lämpligt för hemmanätverk som ej har en autentiseringsserver. Det finns en risk med delad statisk nyckel, just för att den är statisk. Den kan knäckas om man lyssnar på nätverket ett tag och har rätt

verktyg. Risken bedöms till rätt liten dock. Välj därför en så lång nyckel som möjligt (mellan 8 och 63 tecken) och med så slummässiga tecken som möjligt (siffror, bokstäver, specialtecken). Nyckeln skall såklart hållas hemlig och det skadar inte att byta ut den då och då.

TKIP (WPA) = Krypteringsprotokoll för kryptering av dataöverföringen. Kryptering sker med RC4 strömchiffer. WPA med TKIP kallas ibland för WPA 1.

AES (WPA) = Krypteringsprotokoll för kryptering av dataöverföringen. Kryptering sker med Rijndael blockchiffer, som är en starkare krypteringsalgoritm än RC4. WPA med AES kallas ibland WPA 2. Stöd i äldre accesspunkter saknas.

802.11x/EAP = Autentiseringsstandard, som kräver autentiseringsserver (ej för hemmabruk med andra ord).

Nyckelindex = Stöd för flera olika nycklar; Om man har flera datorer och vill ha olika nycklar till dessa.

MAC = Lås accesspunkt mot hårdvaruadressen (MAC) på det trådlösa nätverkskortet i datorn.

SSID = Namnet på det trådlösa nätverket.

Nätverksannonsering = Stäng gärna av annonsering av nätverkets SSID. Datorn måste då känna till exakta SSID-namnet.

Sändareffekt = Accesspunkter har vanligtvis rundstrålande antenner. Minska effekten på sändaren (stöds inte av alla accesspunkter), så når signalen inte till grannarna.