

## SÄKERHETSASPEKTER I SAMBAND MED SKIPTRIPS VIDEOMÖTEN

Ett antal systemlösningar bidrar till att du kan känna dig trygg med att det som sägs under ditt möte inte avlyssnas eller sprids till obehöriga. Det här dokumentet beskriver översiktligt de åtgärder som Skiptrip vidtagit för att förhindra obehörig åtkomst till den information och kommunikation som förekommer under videomötet.

### 1. ALLMÄNT

Skiptrips säkerhetssystem är utformat för att skydda den information och kommunikation som förekommer under och i anslutning till videomötet. Skyddet skall dels förhindra obehörig avlyssning av möteskommunikationen, vilken utgörs av både ljud- och bildsignaler och datakommunikation, dels skall det förhindra obehörig åtkomst till gästernas bärbara datorer och annan utrustning som ofta innehåller känslig företagsinformation.

Dokumentet kan av säkerhetsskäl inte redogöra för de tekniska lösningarna i detalj.

### 2. SIGNALSÄKERHET

#### 2.1 EGET FIBERNÄTVERK FÖR KOMMUNIKATION

För möten mellan Skiptriprum används inte publikt Internet, utan ett helt privat fibernätverk för kommunikationen. Det är den säkraste och mest pålitliga lösningen för videomöten och den är dessutom mycket driftsäker.

Vid möte mellan ett Skiptriprum och en extern ändrustning på ett företag eller konferensanläggning inrikes eller utrikes sker uppkoppling oftast över publikt Internet, vilket innebär en högre risk än när privata förbindelser används.

#### 2.2 KRYPTERING

Om det är önskvärt kan Skiptrip konfigurera videomötet med signalkryptering. Skiptrips system stödjer H.235 AES Security, d v s 128-bitars kryptering.

### 2.3 LOKAL NÄTVERKSSÄKERHET

Skiptrip har konstruerat ett unikt, switchat nät som möjliggör för gästerna att fritt komma åt Internet via nätverksuttag i rummen, samtidigt som produktionssystemen (bl a videosystemen) ligger på ett helt åtskilt nät.

Det nät som levererar gästernas Internetförbindelse är tydligt avgränsat och kan inte användas för avlyssning av eller intrång i produktionssystemen eller andra gästers datorer.

### 2.4 BRANDVÄGG

Trafiken till och från Internet från rummen är också starkt kontrollerad med hjälp av en brandvägg. Brandväggen ser till att gästen kan surfa tryggt, samtidigt som den förhindrar oegentliga aktiviteter, både sådana som bedrivs inifrån och sådana som bedrivs utifrån.

### 3. VÅRA LOKALER

Det är också viktigt att skydda sig mot sådan avlyssning, manipulation och intrång i systemen som utförs genom olagliga aktiviteter i och omkring möteslokalerna. Skiptrips skydd mot dylikt består dels av en stark sekretess kring bokningar och kundinformation, dels av traditionell fysisk säkerhet runt mötesrummen.

#### 3.1 SEKRETESS

Rummens bokningsschemata är inte offentliga. All bokning sker med krypterad förbindelse som kräver inloggning med användarnamn och lösenord. Det gäller även när kunden bokar via telefon hos Skiptrip eller hos våra återförsäljare. Det här betyder att det inte går att få reda på i förväg när en viss kund skall vara i en viss lokal. Inte ens vår lokalpartner, som driver rummet, vet i förväg vem som skall komma till Skiptriprummet.

Det går också att boka helt anonymt, i vilket fall man endast uppger en giltig E-mailadress och ett kreditkortsnummer.

För att ytterligare öka sekretessen kring när och var ditt möte skall äga rum rekommenderar vi att du undviker att boka möten med en förutsägbar periodicitet, t ex samma plats, tid och datum varje månad.

#### 3.2 INPASSERING

Säkerhet är en viktig faktor när Skiptrip väljer ut en lokalpartner. Alla våra lokalpartners är företag med etablerade säkerhetsrutiner och ett mycket gott skalskydd. På de hotell vi samarbetar med finns bemanning dygnet runt. Några av hotellen har även en egen säkerhetscertifiering - se exempel här intill.

Skiptriprummet är också föremål för särskild passerkontroll, där endast en utvald del av lokalpartnerns personal har tillträde till rummet. De enda utomstående personer som släpps in i rummen är gäster som är förälmälda i Skiptrips bokningssystem.

#### 3.3 KAMERAÖVERVAKNING

Alla Skiptriprum är kameraövervakade. Kameraövervakningen används bl a för att kontrollera att gästerna följer de bestämmelser som gäller i rummen, men även för att upptäcka och säkra bevis vid skadegörelse, tillgrepp av egendom eller andra kriminella handlingar.

Övervakningskamerorna lagrar kontinuerligt undan bilder, både översiktsbilder och identifikationsbilder. Bilderna lagras centralt.

” Clarion Hotel Stockholm är säkerhetscertifierat enligt Safehotels och Pinkerton. Safehotels Alliance är ett internationellt certifierings- och kunskapsföretag för hotell och konferenssäkerhet. Safehotels Alliance certifiering utgår ifrån "The Global Hotel Security Standard"©. För att bli godkänd och därmed erhålla Safehotels Alliance Certifiering, krävs det att en hotell och konferensanläggning håller hög nivå då det gäller både säkerhetsrutiner och utrustning.

Anläggningarna som är certifierade har bra dokumentation på sina säkerhetsrutiner och underhåll av utrustning samt välutbildad personal.

Läs mer på [www.safehotels.se](http://www.safehotels.se).