Kommentarer – Vägledning för grundläggande kryptering

Namn: Säkerhets- och försvarsföretagen, SOFF (www.soff.se)

ID	Identifierad förbättringsmöjlighet	Förslag på hur detta kan lösas	Kommentar	Omhändertaget på vilket sätt
	Övergripande			**(Kolumnen ifylls av MSB)**
1	SOFF välkomnar MSB:s initativ för det som ej rör Sveriges säkerhet. Marknaden svämmas över av säkra lösningar och det kan vara svårt att navigera i vad som ger tillräckligt skydd och samtidigt är enkelt att arbeta med.			
2	Målgruppen IT-säkerhetsansvariga bör kunna ha stor nytta av vägledningen och SOFF anser att den är lättbegriplig och välstrukturerad.	SOFF ser en avsaknad av aspekten systemsäkerhet. Bara för att en komponent uppfyller rekommendationen så ger inte det automtiskt ett säkert system. Här rekommenderar SOFF att man utöver vägledningen tar fram ett metodstöd. Metodstödet bör ha sin utgångspunkt i tillgångar, värdet av dessa och hoten mot dem.	I det fall det inte görs riskerar vi att få lösningar som är onödigt dyra eller bristfälliga.	
3	I vägledningen kapitel 6.2 ”Rekommenderade kryptografiska protokoll” ser SOFF vägledningen som begränsande då t.ex. TLS kan användas som VPN.	Denna del kommer att utvecklas i takt med att utvecklingen går framåt och bör revideras kontinuerligt.		

4	Då säkerhet i en lösning beror av hur lösningen är implementerad så bör det finnas sätt att kvalitetssäkra lösningen.		Har lösningen redan en certifiering och vilken typ av certifiering skall då gälla som vägledning? Ser man att MSB kommer att lista rekommenderade lösningar?	
8	4.3.7 Resonemangstext	Det bör finnas ett resonemang som tar upp om admin alltid ska ha tillgång till kryptonycklarna. Ibland kan det vara så att fler användare, andra än admin ska ha access till kryptonycklarna. Det bör alltid vara fler än en om man vill att den krypterade informationen ska kunna ”räddas” om det händer nyckelägaren något. Ska man alltid ha en recovery key? Det bör resoneras huruvida det ska finnas en recovery key eller om informationen hellre ses förlorad än att den kommer i fel händer.		
9	4.3.7.1	Det bör kanske rekommenderas att personal som har access till känslig information ska säkerhetsklassas.		
12	4.3.8.2	Texten ”Utrustning som installerats och konfigurerats med en kryptonyckel (eng. in a keyed state)” är otydlig.		

		Menas utrustning med aktiverad nyckel?		
13	5.4.6 Resonemangstext	Texten ”3DES får inte användas med endast en nyckel, vilket är synonymt med DES.” är inkonsekvent med texten i rekommendationen. Där står det an endast 3DES med tre olika nycklar ska användas. Om inte två nycklars 3DES ska användas så borde det stå i resonemangstexten också.		
17	7.3.2.1 Rekommendationstext	Borde det inte stå "perfect forward secrecy (PFS)"?		
18	8.3.2.2 Rekommendationstext	Det borde beskrivas några lämpliga tekniska åtgärder åtminstone i resonemangsdelen.		
19	8.3.2.3 Rekommendationstext	Det borde pekas ut var man kan hitta information om vad som kan anses vara starka lösenord vad avser komplexitet och längd.		
21	10.3.1.1 Rekommendationstext	Vad har denna rekommendation att göra med hur man hanterar att certifikat eller nycklar röjts? Det borde finnas en massa att skriva om PGP:s nyckelhantering, web of trust.		