Transportstyrelsens författningssamling

TRANSPORT STYRELSEN

Transportstyrelsens föreskrifter om hantering av krypteringsnycklar och certifikat för tillverkning av digitala färdskrivare;

TSFS 2013:1

Utkom från trycket
den 9 januari 2013

VÄGTRAFIK

beslutade den 13 december 2012.

Transportstyrelsen föreskriver följande med stöd av 10 kap. 16 § förordningen (2004:865) om kör- och vilotider samt färdskrivare, m.m.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Dessa föreskrifter innehåller bestämmelser om ansökan om godkännande samt hantering av krypteringsnycklar och certifikat för tillverkning av digitala färdskrivare.

2 § De beteckningar som används i föreskrifterna har samma betydelse som anges i förordningen (2004:865) om kör- och vilotider samt färdskrivare, m.m. och rådets förordning (EEG) nr 3821/85 av den 20 december 1985 om färdskrivare vid vägtransporter[1].

2 kap. Ansökan om godkännande av tillverkningsprocess

1 § En ansökan om godkännande av tillverkning av färdskrivare ska innehålla uppgifter om vilken typ av utrustning som kommer att användas vid tillverkningen och hur informationssäkerhetskraven i 3 kap. ska uppfyllas.

2 § Ett godkännande är giltigt tills vidare eller tills Transportstyrelsen återkallar godkännandet.

3 § Om sökanden avser att väsentligt förändra sin tillverkningsprocess med tillhörande dokumenterade rutiner, eller det som godkännandet omfattar, ska ändringarna först godkännas av Transportstyrelsen.

[1] EGT L 370, 31.12.1985, s. 8 (Celex 31985R3821).

3 kap. Ledningssystem för informationssäkerhet

1 § En färdskrivartillverkare ska ha dokumenterade rutiner i form av ett ledningssystem för informationssäkerhet som motsvarar ISO/IEC 27001. Ledningssystemet ska minst uppfylla de krav som anges i 2–10 §§.

2 § Det ska finnas en person som är ansvarig för ledningssystemet för informationssäkerhet och dess efterlevnad. Den personen ska ha tillräckliga befogenheter för att ledningssystemet för informationssäkerhet ska kunna upprätthållas.

3 § Ledningssystemet ska baseras på en riskanalys som omfattar tillverkning och hantering av färdskrivare. Identifierade risker och åtgärder ska dokumenteras och det ska finnas en rutin för kontinuerlig riskhantering. Riskanalysen ska uppdateras minst en gång var tolfte månad eller vid större ändringar.

4 § En färdskrivartillverkare ska kontinuerligt uppdatera och periodiskt revidera ledningssystemet, dock minst en gång var tolfte månad.

5 § En färdskrivartillverkare ska följa en informationssäkerhetspolicy för tillverkningen där färdskrivartillverkarens arbete med informationssäkerhet är dokumenterat.

6 § En färdskrivartillverkare ska utöver vad som sägs i 2 § ha en organisation som är informationssäkerhetsmässigt lämplig för verksamheten och med tydligt definierade roller och ansvarsfördelning särskilt avseende hanteringen av krypteringsnycklar. Tillverkaren ska se till att personalen har tillräcklig kompetens och förståelse för den tilldelade rollen, samt i övrigt är lämpad för denna.

7 § En färdskrivartillverkare ska dokumentera en klassificering av relevanta informationstillgångar. Klassificeringen ska minst identifiera informationstillgångar som är hemliga, respektive kritiska för tillverkningen.

Färdskrivartillverkaren ska dokumentera hur den säkerställer sekretess, integritet, tillgänglighet och spårbarhet för informationstillgångarna.

8 § En färdskrivartillverkare ska ha en dokumenterad kontinuitetsplan, som beskriver tillverkarens system för förebyggande av oplanerade händelser och akuta åtgärder för att minimera konsekvenserna av sådana händelser.

Säkerhetsincidenter

9 § En färdskrivartillverkare ska ha dokumenterade rutiner för hantering av säkerhetsincidenter. Resultatet av incidenthanteringen ska användas i riskhanteringen.

10 § En färdskrivartillverkare ska rapportera säkerhetsincidenter som rör krypteringsnycklar och färdskrivarcertifikat till Transportstyrelsen.

Lagring av information

11 § En tillverkare av fordonsenheter ska spara färdskrivarcertifikat och serienummer för varje fordonsenhet som tillverkas, samt annan information som bidrar till att utrustningen kan spåras.

12 § En tillverkare av fordonsenheter ska spara information som gör det möjligt att spåra vilka personer som hanterat krypteringsnycklar och certifikat när en färdskrivare tillverkas.

13 § En tillverkare av rörelsegivare ska spara rörelsegivarens utökade serienummer (Ns och Kp) för varje rörelsegivare som tillverkats, samt annan information som bidrar till att utrustningen kan spåras.

14 § Informationen i 11–13 §§ ska på begäran lämnas till Transportstyrelsen.

4 kap. Tillverkning av färdskrivare, hantering av krypteringsnycklar och certifikat

Framställning av RSA-nycklar

1 § Färdskrivartillverkaren ska framställa RSA-nycklar på ett säkert sätt. Ingen obehörig person ska kunna komma åt en fordonsenhets privata nyckel och den ska heller inte kunna förvanskas.

2 § RSA-nycklar ska framställas i en utrustning som

– uppfyller kraven enligt nivå 3 i FIPS 140–2, 140–1,

– uppfyller kraven i CEN Workshops överenskommelse 14167–2:2002 eller motsvarande,

– är certifierad enligt EAL 4 eller högre i enligt med Common Criteria (ISO 15408:1999), säkerställt med E3 eller högre i ITSEC version 1.2 eller högre, eller

– uppfyller likvärdiga säkerhetskrav.

Slumptalsgeneratorn för framställning av nycklar ska ha en sådan kvalitet att risken för framställning av nycklar som inte är unika är försumbar.

3 § RSA-nycklar som framställts enligt tillägg 11:2.2.1/3.2, bilaga 1 B till rådets förordning (EEG) nr 3821/85 av den 20 december 1985 om färdskrivare vid vägtransporter ska skyddas mot förvanskning.

4 § Om nycklar framställs utanför fordonsenheten ska tillverkaren radera den privata nyckeln ur det fristående nyckelframställningssystemet när nyckeln installeras i fordonsenheten. Om fordonsenhetens privata nyckel

måste lagras innan den kan installeras i fordonsenheter ska detta ske på ett sådant sätt att nyckeln hålls hemlig och inte kan förvanskas.

Lagring av RSA-nycklar

5 § Lagring av privata nycklar ska ske i en utrustning som
– uppfyller kraven enligt nivå 3 i FIPS 140–2, 140–1,
– är certifierad enligt EAL 4 eller högre i enligt med Common Criteria (ISO 15408:1999), säkerställt med E3 eller högre i ITSEC version 1.2 eller högre, eller
– uppfyller likvärdiga säkerhetskrav.

Privata nyckar får endast lagras hos färdskrivartillverkaren.

Hantering och lagring av den europeiska publika nyckeln och rörelsegivarnyckeln

6 § Färdskrivartillverkaren ska hantera den europeiska publika nyckeln så att den inte kan förvanskas.

7 § Färdskrivartillverkaren ska hantera rörelsegivarnyckeln (KmVU) så att den hålls hemlig och inte kan förvanskas.

8 § Rörelsegivarnyckeln ska lagras i en utrustning som
– uppfyller kraven enligt nivå 3 i FIPS 140–2, 140–1,
– är certifierad enligt EAL 4 eller högre i enligt med Common Criteria (ISO 15408:1999), säkerställt med E3 eller högre i ITSEC version 1.2 eller högre, eller
– uppfyller likvärdiga säkerhetskrav.

Färdskrivarcertifikat

9 § För varje fordonsenhet ska tillverkaren sammanställa en certifikatbegäran för färdskrivarcertifikat. Begäran ska innehålla en unik referens till fordonsenheten samt en öppen nyckel som motsvarar den privata nyckel som hör till fordonsenheten. Genom begäran intygar tillverkaren att varje publik nyckel har en motsvarande privat nyckel. Begäran ska skyddas mot förvanskning.

En certifikatbegäran ska överföras elektroniskt till Transportstyrelsen på det sätt som Transportstyrelsen anger.

10 § Innan färdskrivarcertifikatet installeras i fordonsenheten ska tillverkaren kontrollera att det kommer från Transportstyrelsen.

Hantering av rörelsegivare

11 § Färdskrivartillverkaren ska lämna rörelsegivarens utökade serienummer (Ns och Kp) för kryptering med rörelsegivarnyckeln (Km) till Transportstyrelsen genom elektronisk överföring på det sätt som Transportstyrelsen anger.

12 § Innan rörelsegivarens krypterade utökade serienummer (Ns och Kp) installeras i rörelsegivaren ska tillverkaren kontrollera att det kommer från Transportstyrelsen.

5 kap. Åtgärder om krypteringsnycklar avslöjats samt kassering av fordonsenhet vid tillverkning och när tillverkning upphör

Om en krypteringsnyckel avslöjats

1 § Finns det skäl att tro att den symmetriska rörelsegivarnyckeln (KmVU) eller den privata nyckeln för färdskrivarens fordonsenhet avslöjats för obehörig person ska tillverkaren utan dröjsmål meddela Transportstyrelsen detta.

2 § Om den privata nyckeln avslöjats ska färdskrivartillverkaren vidta åtgärder för att förhindra att fordonsenheten tas i bruk.

Kassering av fordonsenhet

3 § Om krypteringsnycklar har installerats i en fordonsenhet som därefter inte färdigställs eller av annan orsak inte tas i bruk ska tillverkaren förstöra krypteringsnycklarna i enheten innan fordonsenheten kasseras.

Åtgärder vid tillverkningens upphörande

4 § Upphör en färdskrivartillverkare med tillverkning av digitala färdskrivare ska samtliga kopior av rörelsegivarnyckeln (KmVU) förstöras samt den information som avses i 3 kap. 11–13 §§ överföras till Transportstyrelsen på det sätt som Transportstyrelsen anger.

6 kap. Undantag

1 § Undantag från dessa föreskrifter prövas av Transportstyrelsen.

Denna författning träder i kraft den 1 februari 2013 då Vägverkets föreskrifter (VVFS 2005:79) om hantering av nycklar och certifikat för tillverkning av digitala färdskrivare ska upphöra att gälla.

På Transportstyrelsens vägnar

STAFFAN WIDLERT

Arne Classson
Väg- och järnvägsavdelningen

Utgivare: Kristina Nilsson, Transportstyrelsen, Norrköping ISSN 2000-1975