Transportstyrelsens författningssamling

TRANSPORT STYRELSEN

TSFS 2018:85

Utkom från trycket
den 25 september 2018

VÄGTRAFIK

# Transportstyrelsens föreskrifter om hantering av kryptografiska nycklar och certifikat med mera för tillverkning av digitala färdskrivare;

beslutade den 14 september 2018.

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

## Inledande bestämmelser

### Tillämpningsområde

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

### Definitioner

**2 §** De beteckningar som används i föreskrifterna har samma betydelse som i

– kommissionens genomförandeförordning (EU) 2016/799 av den 18 mars 2016 om genomförande av Europaparlamentets och rådets förordning (EU) nr 165/2014 när det gäller krav för konstruktion, provning, installation, drift och reparation av färdskrivare och deras komponenter,

– Europaparlamentets och rådets förordning (EU) nr 165/2014 av den 4 februari 2014 om färdskrivare vid vägtransporter, om upphävande av rådets förordning (EEG) nr 3821/85 om färdskrivare vid vägtransporter och om ändring av Europaparlamentets och rådets förordning (EG) nr 561/2006 om harmonisering av viss sociallagstiftning på vägtransportområdet, och

– förordningen (2004:865) om kör- och vilotider samt färdskrivare, m.m.

## Godkännande av tillverkningsprocessen

**3 §** En ansökan om godkännande av tillverkning av färdskrivare ska innehålla uppgifter om vilken typ av utrustning som kommer att användas vid tillverkningen, typgodkännande och hur informationssäkerhetskraven i 6–9 §§ ska uppfyllas.

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

**5 §** Om tillverkaren avser att väsentligt förändra sin tillverkningsprocess, ska detta rapporteras till Transportstyrelsen. Ändringarna får inte genomföras innan Transportstyrelsen godkänt den nya processen.

## Ledningssystem för informationssäkerhet

**6 §** En tillverkare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete som motsvarar kraven för ledningssystem i ISO/IEC 27001. Ledningssystemet ska vid förändringar av betydelse uppdateras och periodiskt granskas, dock minst en gång var tolfte månad.

**7 §** Ledningssystemet ska baseras på en riskanalys som omfattar tillverkning och hantering av färdskrivarkomponenter. 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.

**8 §** Det ska finnas en person som är ansvarig för ledningssystemet för informationssäkerhet och dess efterlevnad. Denne ska ha tillräckliga befogenheter för att ledningssystemet för informationssäkerhet ska kunna upprätthållas.

**9 §** Tillverkaren ska utan dröjsmål rapportera säkerhetsincidenter som rör kryptografiska nycklar och certifikat till Transportstyrelsen.

## Lagring av information

**10 §** En tillverkare av fordonsenheter ska spara certifikat och serienummer för varje fordonsenhet som tillverkas samt annan information som bidrar till att utrustningen kan spåras. Vid tillverkningen ska information sparas som gör det möjligt att spåra de personer som hanterat kryptografiska nycklar och certifikat. Informationen ska även omfatta datum och klockslag. Den ska på begäran lämnas till Transportstyrelsen.

**11 §** En tillverkare av rörelsesensor ska spara rörelsesensorns serienummer och parningsnyckel för varje rörelsesensor som tillverkas samt annan information som bidrar till att utrustningen kan spåras. Vid tillverkningen ska information sparas som gör det möjligt att spåra vilka personer som hanterat serienumren och parningsnycklarna. Informationen ska även omfatta datum och klockslag. Informationen ska på begäran lämnas till Transportstyrelsen.

**12 §** En tillverkare av externa GNSS-anordningar ska spara certifikat och serienummer för varje anordning som tillverkas samt annan information som bidrar till att utrustningen kan spåras. Vid tillverkningen ska information sparas som gör det möjligt att spåra vilka personer som hanterat certifikaten. Informationen ska även omfatta datum och klockslag. Den ska på begäran lämnas till Transportstyrelsen.

## Hantering av kryptografiska nycklar och certifikat

### Tillverkning, hantering och lagring av privata nycklar

**13 §** Tillverkaren ska tillverka och hantera privata nycklar på en säker plats. Ingen obehörig ska kunna komma åt nycklarna och dessa ska inte heller kunna förvanskas.

**14 §** Nycklarna till smarta färdskrivare eller andra generations färdskrivare ska tillverkas och lagras i en utrustning som

1. uppfyller kraven enligt nivå 3 i FIPS PUB 140–2,
2. uppfyller kraven i ISO/IEC 19790 nivå 3,
3. är certifierad enligt EAL 4 eller högre i enlighet med ISO 15408, och där lösningen följer en lämplig skyddsprofil, eller
4. uppfyller säkerhetskrav i enlighet med nationella eller internationellt likvärdiga erkända utvärderingskriterier för it-säkerhet.

Slumptalsgeneratorn för tillverkning av nycklar ska vara av sådan kvalitet att risken för att nycklar inte blir unika är försumbar.

**15 §** Nycklarna till digitala färdskrivare eller första generations färdskrivare ska tillverkas och lagras i en utrustning som

1. uppfyller kraven enligt nivå 3 i FIPS 140–2, 140–1,
2. uppfyller kraven i CEN Workshops överenskommelse 14167–2,
3. är certifierad enligt EAL 4 eller högre i enlighet med Common Criteria (ISO 15408:1999), säkerställt med E3 eller högre i ITSEC version 1.2 eller högre, eller
4. uppfyller likvärdiga säkerhetskrav enligt 1, 2 eller 3.

Slumptalsgeneratorn för tillverkning av nycklar ska vara av sådan kvalitet att risken för att nycklar inte blir unika är försumbar.

**16 §** Om nycklarna kan tillverkas av färdskrivaren ska tillverkningen täckas av färdskrivarens säkerhetscertifiering.

**17 §** Om nycklar tillverkas utanför färdskrivaren, ska tillverkaren radera de privata nycklarna ur det fristående nyckelframställningssystemet när nycklarna installeras i färdskrivaren. Om färdskrivarens nycklar måste lagras innan de kan installeras, ska detta ske på ett sådant sätt att dessa nycklar hålls hemliga och inte kan förvanskas.

**18 §** Nycklarna får endast lagras hos tillverkaren och endast till dess att de installerats i en fordonsenhet eller en extern GNSS-anordning.

**19 §** Tillverkaren ska ha dokumenterade rutiner om tillverkning, hantering och lagring av nycklar.

### Hantering och lagring av symmetriska huvudnycklar

**20 §** Tillverkaren ska hantera och lagra symmetriska huvudnycklar på en säker plats. Ingen obehörig ska kunna komma åt nycklarna och de ska inte heller kunna förvanskas.

**21 §** Tillverkaren ska ta emot nycklarna på det sätt som Transportstyrelsen anger.

**22 §** Nycklarna till smarta färdskrivare eller andra generations färdskrivare ska lagras i en utrustning som

1. uppfyller kraven enligt nivå 3 i FIPS PUB 140–2,
2. uppfyller kraven i ISO/IEC 19790 nivå 3,
3. är certifierad enligt EAL 4 eller högre i enlighet med ISO 15408, och där lösningen följer en lämplig skyddsprofil, eller
4. uppfyller säkerhetskrav i enlighet med nationellt eller internationellt likvärdiga erkända utvärderingskriterier för it-säkerhet.

**23 §** Nycklarna till digitala färdskrivare eller första generations färdskrivare ska lagras i en utrustning som

1. uppfyller kraven enligt nivå 3 i FIPS 140–2, 140–1,
2. är certifierad enligt EAL 4 eller högre i enlighet med Common Criteria (ISO 15408:1999), säkerställt med E3 eller högre i ITSEC version 1.2 eller högre, eller
3. uppfyller likvärdiga säkerhetskrav enligt 1 eller 2.

**24 §** Nycklarna får endast hanteras då två personer närvarar.

**25 §** Tillverkaren ska ha dokumenterade rutiner om hantering och lagring av nycklar.

### Certifikat

**26 §** För varje fordonsenhet eller extern GNSS-anordning ska tillverkaren sammanställa en certifikatbegäran. En certifikatbegäran ska utformas och översändas elektroniskt till Transportstyrelsen på det sätt Transportstyrelsen anger.

**27 §** Innan certifikatet installeras i fordonsenheten eller den externa GNSS-anordningen ska tillverkaren kontrollera att det kommer från Transportstyrelsen.

**28 §** Tillverkaren ska ha dokumenterade rutiner om hanteringen av certifikat.

### Hantering av rörelsesensordata

**29 §** Tillverkaren ska tillverka och hantera parningsnycklar på en säker plats. Ingen obehörig ska kunna komma åt nycklarna och de ska inte heller kunna förvanskas.

**30 §** Nycklarna till smarta färdskrivare eller andra generations färdskrivare ska tillverkas och lagras i en utrustning som

1. uppfyller kraven enligt nivå 3 i FIPS PUB 140–2,
2. uppfyller kraven i ISO/IEC 19790 nivå 3,
3. är certifierad enligt EAL 4 eller högre i enlighet med ISO 15408, och där lösningen följer en lämplig skyddsprofil, eller
4. uppfyller säkerhetskrav i enlighet med nationella eller internationellt likvärdiga erkända utvärderingskriterier för it-säkerhet.

Slumptalsgeneratorn för tillverkning av nycklar ska vara av sådan kvalitet att risken för att nycklar inte blir unika är försumbar.

**31 §** Nycklarna till digitala färdskrivare eller första generations färdskrivare ska tillverkas och lagras i en utrustning som

1. uppfyller kraven enligt nivå 3 i FIPS 140–2, 140–1,
2. uppfyller kraven i CEN Workshops överenskommelse 14167–2,
3. är certifierad enligt EAL 4 eller högre i enlighet med Common Criteria (ISO 15408:1999), säkerställt med E3 eller högre i ITSEC version 1.2 eller högre, eller
4. uppfyller likvärdiga säkerhetskrav enligt 1, 2 eller 3.

Slumptalsgeneratorn för tillverkning av nycklar ska vara av sådan kvalitet att risken för att nycklar inte blir unika är försumbar.

**32 §** Tillverkaren ska överföra rörelsesensorns serienummer och parningsnyckel för kryptering till Transportstyrelsen på det sätt som Transportstyrelsen anger.

**33 §** Innan rörelsesensorns krypterade serienummer och parningsnyckel installeras i rörelsesensorn ska tillverkaren kontrollera att de kommer från Transportstyrelsen.

**34 §** Tillverkaren ska ha dokumenterade rutiner om hanteringen av serienummer och parningsnycklar.

### Hantering av data för K_VU$_{DSRC}$_ENC och K_VU$_{DSRC}$_MAC

**35 §** Tillverkaren ska hantera och lagra K_VUDSRC_ENC och K_VUDSRC_MAC på en säker plats. Ingen obehörig ska kunna komma åt K_VUDSRC_ENC och K_VUDSRC_MAC och de ska inte heller kunna förvanskas.

**36 §** Tillverkaren av fordonsenheter ska överföra fordonsenhetens serienummer till Transportstyrelsen på det sätt som Transportstyrelsen anger.

**37 §** Innan K_VUDSRC_ENC och K_VUDSRC_MAC installeras i fordonsenheten ska tillverkaren kontrollera att de kommer från Transportstyrelsen.

**38 §** Tillverkaren ska ha dokumenterade rutiner om hanteringen av data för K_VUDSRC_ENC och K_VUDSRC_MAC.

## Åtgärder vid röjning av kryptografiska nycklar, kassering av färdskrivare vid tillverkning och när tillverkning upphör

### Om en kryptografisk nyckel röjs

**39 §** Om det finns anledning att anta att någon av de symmetriska huvudnycklarna eller privata nycklarna röjts för obehörig person ska tillverkaren utan dröjsmål meddela Transportstyrelsen detta.

**40 §** Tillverkaren ska ha dokumenterade rutiner om hur röjda kryptografiska nycklar ska hanteras. I rutinen ska ingå de åtgärder som ska vidtas för att förhindra att färdskrivaren tas i bruk.

### Kassering av färdskrivare som inte färdigställts

**41 §** Om kryptografiska nycklar har installerats i en färdskrivare som därefter inte färdigställs eller av annan orsak inte tas i bruk, ska tillverkaren förstöra nycklarna i enheten innan färdskrivaren kasseras.

**42 §** Tillverkaren ska ha dokumenterade rutiner om hur färdskrivare som inte färdigställts ska kasseras.

### Åtgärder vid tillverkningens upphörande

**43 §** Om en tillverkare upphör med tillverkning av färdskrivare ska samtliga kopior av de symmetriska huvudnycklarna förstöras och information enligt 10–12 §§ överföras till Transportstyrelsen på det sätt som Transportstyrelsen anger.

**44 §** Undantag från dessa föreskrifter prövas av Transportstyrelsen.

---

1. Denna författning träder i kraft den 15 oktober 2018
2. Genom denna författning upphävs Transportstyrelsens föreskrifter (TSFS 2013:1) om hantering av nycklar och certifikat för tillverkning av digitala färdskrivare

På Transportstyrelsens vägnar

JONAS BJELFVENSTAM

Pernilla Lindblom
(Väg och järnväg)

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