

**Upute za implementaciju sigurnog komunikacijskog kanala za prijenos elektroničkih zrakoplovnih podataka**

**Instructions for implementing a secure communication channel for transfer of electronic aeronautical data**

**Naredba o zrakoplovnoj sigurnosti: ASO-2012-002**

**Air Safety Order: ASO-2012-002**

Pokretač: Agencija za civilno zrakoplovstvo

Initiated by: Croatian Civil Aviation Agency

**Područje primjene:**

Naredba o zrakoplovnoj sigurnosti se odnosi na zračne luke, Hrvatsku kontrolu zračne plovidbe d.o.o. te Agenciju za civilno zrakoplovstvo u skladu sa odredbom članka 10. Pravilnika o aerodromima ("Narodne novine" br. 64/10).

**Area of application:**

*This Air Safety Order (hereinafter: ASO) is applicable to the airports, Croatia Control Ltd. and Croatian Civil Aviation Agency, pursuant to article 10. of Ordinance on aerodromes (Official Gazette, No. 64/10).*

**Referentni propisi:**

- Pravilnik o aerodromima („Narodne novine“ br. 64/10).

**Regulation Reference:**

- Ordinance on aerodromes (Official Gazette, No. 64/10)

**Svrha:**

Ova Naredba o zrakoplovnoj sigurnosti izdana je u svrhu utvrđivanja postupaka i kriterija za osiguranje cjelovitosti zrakoplovnih podataka dok su pohranjeni ili prilikom njihova prenošenja, u skladu sa člankom 10. Pravilnika o aerodromima.

**Purpose:**

*This ASO is published in order to establish procedures and criteria for ensuring the integrity and protection of electronic aeronautical data while stored or in transit, pursuant to article 10. of the Ordinance on aerodromes.*

**1. Uvod**

Obzirom da se prijenos dijela zrakoplovnih podataka između zračnih luka, Hrvatske kontrole zračne plovidbe d.o.o. i Agencije za civilno zrakoplovstvo obavlja putem elektronske pošte (e-maila), pošiljalatelj i primatelj moraju podesiti svoje mail poslužitelje (servere) na način da se osigura siguran komunikacijski kanal za prijenos podataka.

**1. Background**

*Considering that one part of data transfer between airports, Croatia Control Ltd. and Croatian Civil Aviation Agency is carried out through e-mail service, the sender and receiver must adjust their mail servers to ensure a secure communication channel for the transmission of data.*

**Članak 10., stavak 3. Pravilnika o aerodromima:**

Zaštita elektroničkih zrakoplovnih podataka dok su pohranjeni ili se prenose, biti će utemeljena na sustavu provjere cikličke zalihosti (cyclic redundancy check – CRC). Pri tome, u zaštiti cjelovitosti:

- a) kritičnih i bitnih podataka, primjenjuje se 32-bitni, ili 24-bitni algoritam CRC-a
- b) rutinskih podataka, primjenjuje se 16-bitni algoritam CRC-a.

**The article 10. paragraph 3. of Ordinance on aerodromes:**

*Protection of electronic aeronautical data while stored or in transit shall be totally monitored by the cyclic redundancy check (CRC):*

- a) *To achieve protection of the integrity level of critical and essential aeronautical data, a 32- or 24-bit CRC algorithm shall apply respectively*
- b) *To achieve protection of the integrity level of routine aeronautical data, a 16-bit CRC algorithm shall apply*

## 2. Implementacija

1. Ukoliko pošiljatelj i primatelj elektroničkih zrakoplovnih podataka imaju sigurni mail poslužitelj (server), za zaštitu zrakoplovnih podataka koji se prenose elektroničkim putem (putem e-maila) prilikom prijena moraju:

- a) koristiti pristupne postavke sigurnog (secure) mail poslužitelja (servera). Podaci o sigurnom mail poslužitelju mogu se dobiti od pružatelja mail usluga.

Incoming mail server:	<input type="text" value="ime.sigurnog.servera"/>
Outgoing mail server (SMTP):	<input type="text" value="ime.sigurnog.servera"/>

- b) implementirati 32-bitnu enkripciju na način da se instaliraju sigurnosni certifikati (CA-Certificate Authority, Digital ID) na postojeću računalnu mrežu.

2. Ako pošiljatelj i primatelj elektroničkih zrakoplovnih podataka nemaju sigurni mail poslužitelj (server), onda ostaju postavke „običnog“ mail poslužitelja (servera):

- a) koristiti SSL konekciju/protokol za dolazni (Incoming) i odlazni (Outgoing) mail server

Internet E-mail Settings

General | Outgoing Server | Connection | **Advanced**

Server Port Numbers

Incoming server (POP3): 995

This server requires an encrypted connection (SSL)

Outgoing server (SMTP): 465

Use the following type of encrypted connection: **SSL**

Server Timeouts

Short  Long 10 minutes

Delivery

Leave a copy of messages on the server

Remove from server after 3 days

Remove from server when deleted from 'Deleted Items'

- b) implementirati 32-bitnu enkripciju na način da se instaliraju sigurnosni certifikati (CA-Certificate Authority, Digital ID) na postojeću

## 2. Implementation

1. If the sender or receiver of electronic aeronautical data has a secure mail server for the protection of electronic aeronautical data while transferring (through e-mail) then:

- a) Use the access settings of secured mail server. Information on secured mail server should be available from your mail provider.

Incoming mail server:	<input type="text" value="secure.server.name"/>
Outgoing mail server (SMTP):	<input type="text" value="secure.server.name"/>

- b) implement 32-bit encryption in a way to install security certificates (CA-Certificate Authority, Digital ID) to an existing computer network.

2. If the sender or receiver of electronic aeronautical data does not have a secured e-mail server then e-mail settings will remain "normal":

- a) use SSL connection/protocol for incoming and outgoing email server

Internet E-mail Settings

General | Outgoing Server | Connection | **Advanced**

Server Port Numbers

Incoming server (POP3): 995

This server requires an encrypted connection (SSL)

Outgoing server (SMTP): 465

Use the following type of encrypted connection: **SSL**

Server Timeouts

Short  Long 10 minutes

Delivery

Leave a copy of messages on the server

Remove from server after 3 days

Remove from server when deleted from 'Deleted Items'

- b) implement 32-bit encryption in a way to install security certificates (CA-Certificate Authority, Digital ID) to an existing computer network.

računalnu mrežu.

**3. Rok za implementaciju:**

Zračne luke, Hrvatska kontrola zračne plovidbe d.o.o. i Agencija za civilno zrakoplovstvo moraju kupiti certifikat od ovlaštenog prodavatelja sigurnosnog certifikata i implementirati ga do 30.06.2012. godine.

**4. Nadzor**

Nadzor nad primjenom ove Naredbe provodi Agencija za civilno zrakoplovstvo.

**3. Implementation timeframe**

*Airports, Croatia Control Ltd. and Croatian Civil Aviation Agency should purchase a certificate from authorized certificate dealer and implement it not later than 30th June 2012.*

**4. Oversight**

*Supervision over the implementation of this directive is carried out by CCAA.*

U Zagrebu, 15.02.2012.

Za Agenciju za civilno zrakoplovstvo:  
*For Croatian Civil Aviation Agency:*

Omer Pita, dipl.ing.  
Direktor

