hitrail
european railway IT & data communications

Ensuring security and continuity within the Hermes VPN

From GSM-R to FRMCS

Paris, 18-19 May 2017

Enrique Ruiz López

Technical and Service Manager

enrique.ruiz@hitrail.com

heros
HERmes Open Services

Hit Rail : Born to interconnect the Railways

- Hit Rail is a **non-profit making** company, expert in data communications for the European railway environment
- It was created in 1990 to professionally manage the Hermes data network, already in use by the railways **since 1978**
- It has developed an international prestige in guaranteeing a **reliable and up to date service**
- It is a trusted and **neutral Railway sector organisation**
- **Open to all** – fair cost recovery pricing system.

Hit Rail is a company owned by Railways: IMs, RUs

ADIF - Spain
CD – Czech Republic
DSB - Denmark
EVRY - Sweden
FS - Italy
MAV - Hungary
ÖBB - Austria
SBB CFF FFS - Switzerland
SNCB - Belgium
SNCF- France
SZ - Slovenia
ZSR - Slovakia

hitrail
european railway IT & data communications

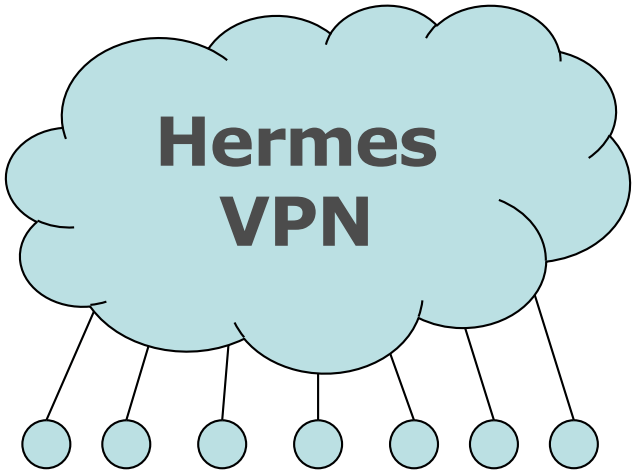
Hit Rail services are used by small and large Railways, newcomers and incumbents, creating the Hermes ecosystem

Adif, ATOC, B-Cargo, Captrain, CD, CD Cargo, CFL, CFR, DB, DB Netz, DB Schenker, DSB, Eurostar, HZ Cargo, HZPP, Infrabel, Inrail, Lokomotion, MAV Start, Network Rail, NMBS/SNCB, NS, ÖBB, PKP Cargo, PKP Intercity, ProRAIL, Raildata, RCA, RCH, Renfe, RFI, RhB, RMF, RNE, RZD, SBB, SBB Cargo, SJ, SNCF, SNCF Fret, TCDD, THALYS, Trenitalia, UIC, UZ, VR, ZS, ZSR, ZSSK, ZSSK Cargo.

Connectivity and Interoperability

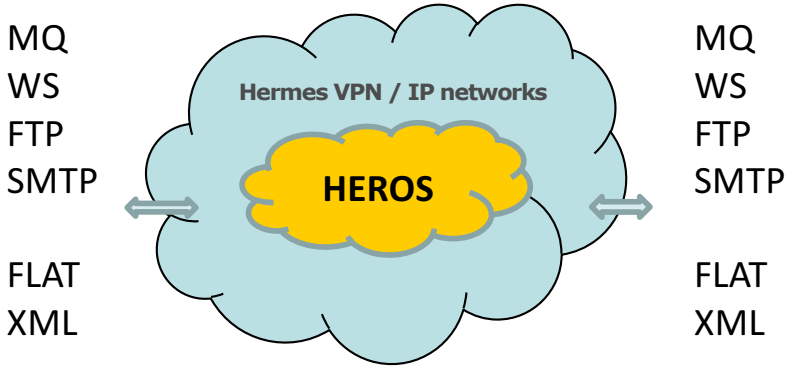
The Hermes Ecosystem offers to the railway community two main services:

Application to application connectivity



One connection to the VPN connects you to all Hermes Railway companies

Interoperability



Messaging translation across channel protocols, file formats, versions

What Hermes does and why it is business critical

- Mainly inter-company (B2B) data communications, few intra-company
- Mainly international RU to RU data telecommunications
- 60% traffic is RU to RU passenger reservations (UIC 918, EPA)
- Freight applications (H30 Freight Pre-advice for RU to RU train handover and border crossing)
- RU - IM communications (Path request, Train running information)
- International train maintenance applications

What happens if our service would fail?

- European RUs and IMs would not be able to cooperate and exchange business messages electronically
- Passengers would not be able to book seats on Hermes partner railways
- Freight trains handovers be significantly delayed at exchange points & country borders

How we ensure continuity and security:
1. MPLS-based core network

hitrail
european railway IT & data communications

The core of the Hermes VPN is a

BT-supplied MPLS-based international IP VPN service

- **MPLS weaves together multiple International networks owned or contracted by BT**
- **The network core from the Hit Rail point of view is rock-solid, with alternative routing and redundant capacity**
- **It provides an inherent secure, highly available and stable service**
- **Fault events involving a loss of the Hermes service are extremely rare!!!**

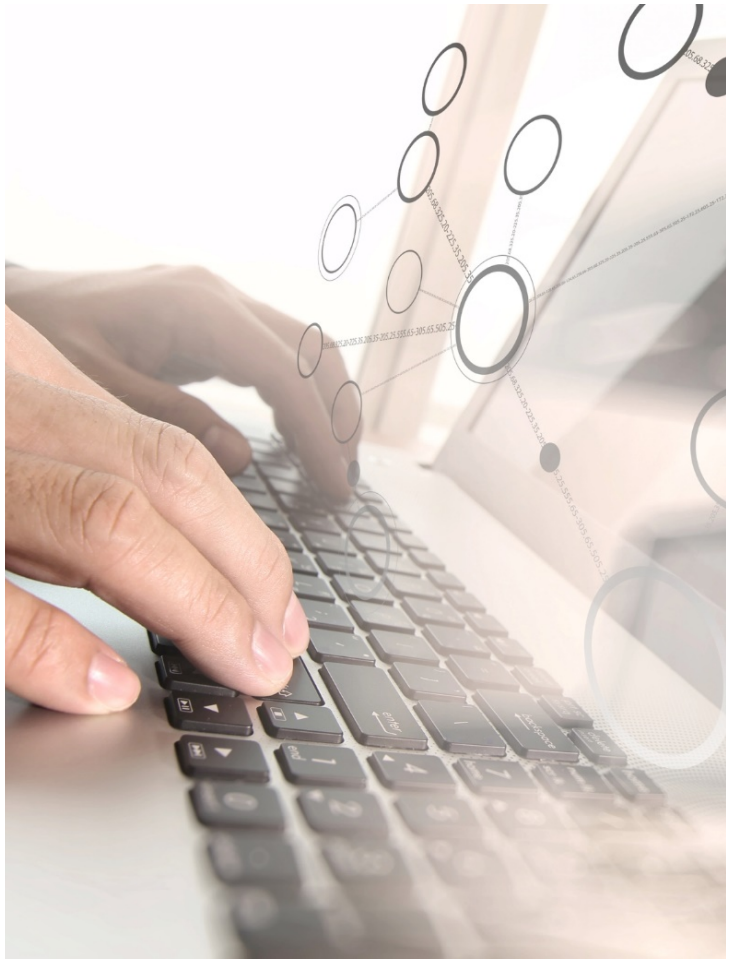
How we ensure continuity and security:
2. Understanding where the risks for uptime are

hitrail
european railway IT & data communications

Network access is where 99% of the faults happen, so access links have to be as fully redundant as possible

Network access technologies used on the Hermes VPN:

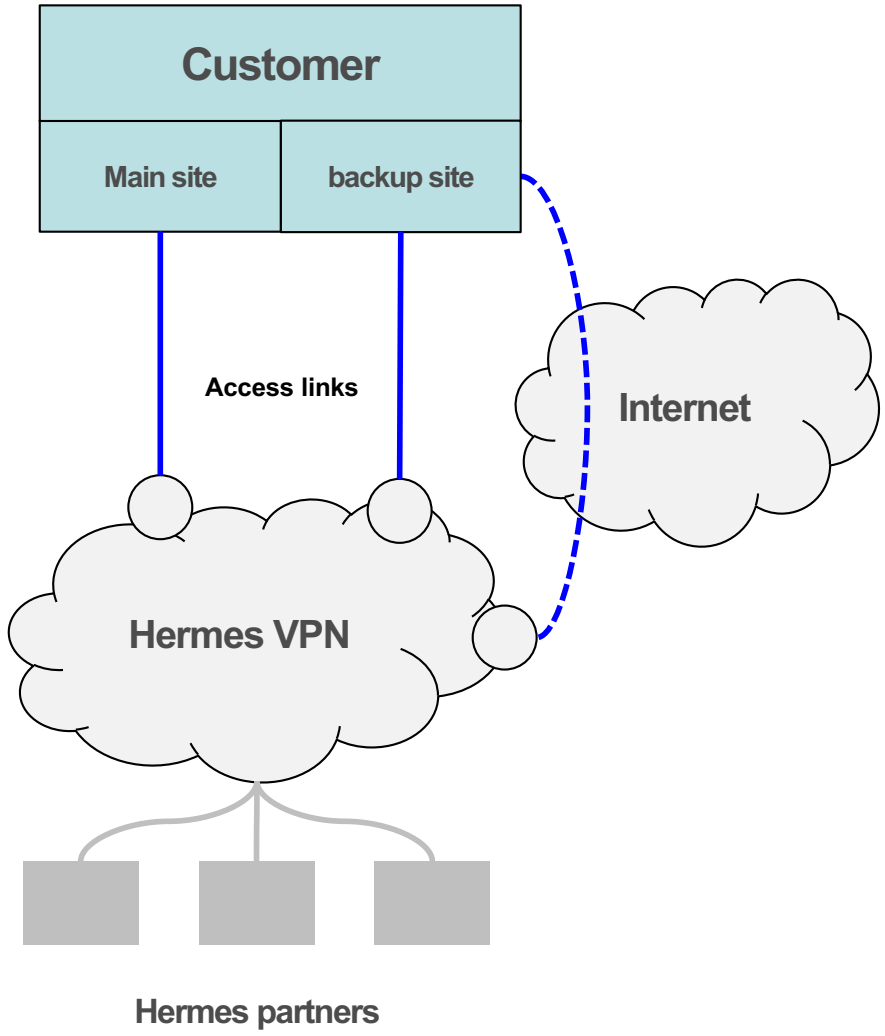
- **Leased lines**
- **Ethernet links**
- **IPsec over the Internet**



How we ensure continuity and security:
3. Bullet-proof network access

- **Separate geographical sites for main and backup sites**
- **One router at each location**
- **Each access link is sourced to a different Telco provider**
- **Each link is connected to a different BT Point of Presence**
- **Use of Internet as additional backup**

Historical 100% uptime on customers with this level or redundancy



How we ensure continuity and security:
4. A collaborative security policy

hitrail
european railway IT & data communications

Why the Hermes VPN is a secure network

- The use of MPLS makes the core network secure:
  - There is no network visibility outside the VPN
  - There are no known threats to MLPS
- Each connected partner is responsible for its own firewall and security rules. Each one takes care of their own door.
- The common Hermes Security Policy is reviewed periodically in collaboration among the members.
- We work together with all our members to achieve the best possible balance between resiliency and cost.

Has Hermes had any network security-related incidents?

- No, in the MPLS network core and dedicated accesses
- Yes, on the Internet. DDOS attacks on some customers' own Internet access have affected their Internet-based access to Hermes.
  - We recommend dedicated access for Hermes, and using Internet only for backup access.

Proactive monitoring and support

24/365 proactive monitoring and support are essential for business critical applications

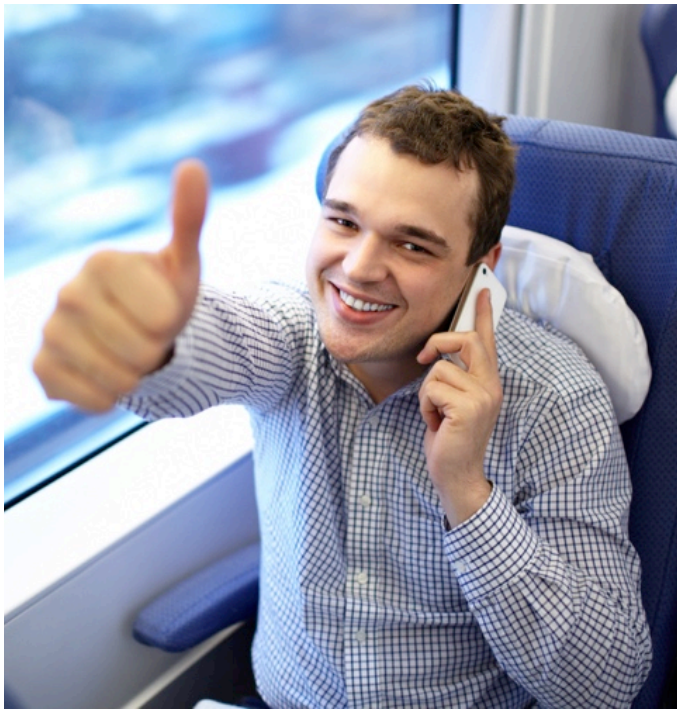
Proactive means that cases are opened before the customer does. The customer is contacted and finds the case open already

Proactive also means coordinating issues across providers and Hermes partners.

We have contacts at different levels (network, firewall application, business) at every Railway partner.

The human factor:

- **First-line support and Service Management are unified.**
- **Your Service Manager knows how you use the service, who your partners are, and how you are impacted.**
- **If there is a fault we tell you where the cause is: network or partner.**



What is the future of Hermes VPN?

hitrail
european railway IT & data communications

We have asked our customers what they want:

- **Same or better performance and reliability at lower prices**
- **…but lower prices never at the expense of lower reliability, performance or support quality**

Many of our customers' applications are business critical, so…

An MPLS-based VPN is our core model at present

<u>The Internet is not ready</u> at present for International business critical applications, because of security, technical and business reasons (SLAs).

The case for the Internet may improve, but for the moment it is limited to smaller users who accept the risks, or for backups.

Thank you for your attention

We connect

the European Railways

Website www.hitrail.com
Contact info@hitrail.com