

# First-class security for Saarland

Authorities and the police use BSI-compliant encryption

Reference project:



**“With this solution, Saarland is not just consistently implementing “cybersecurity first”. It is also providing a template for Germany, showing how complete encryption of all the state’s authorities can be implemented across the board.”**

Ammar Alkassar, CIO for Saarland

Digitalization in Saarland is not just an idea or an opportunity to improve people’s lives. Digitalization is a management issue. Minister-President Tobias Hans has convened a Digitalization Council with experts that is responsible for monitoring Saarland’s digitalization roadmap. New structures were specifically created at the Ministry for Economic Affairs and Labor in order to drive the digital agenda forward. “My vision is for Saarland to become the epitome of digitalization, cyber safety, and artificial intelligence with its Digital Saarland brand,” explains the Minister-President of Saarland, which comprises around one million citizens. In the meantime, Saarland has passed one of the first milestones on the digitalization roadmap. As the IT communication of the state’s authorities is uniformly and strongly encrypted, a secure foundation has been established on which further digitalization can be advanced.

## At a glance

In cooperation with T-Systems as well as security company Rohde & Schwarz Cybersecurity GmbH, Saarland is the first federal state to implement a modern, flexible, and comprehensive encryption of the state authorities in accordance with the BSI (Federal Office for Information Security). This encryption now allows classified information to be exchanged with the note “VS-NfD” (classified – official use only).

- Introduction of high-performance multipoint-to-multipoint encryption
- Customization of the standard solution to meet the requirements of the Saarland IT service center and the police
- Detailed planning and technical coordination of the project by T-Systems
- Saarland as a national “first mover”

# Reference in detail

## The challenge

The state data center at the IT service center (IT-DLZ) in Saarbrücken processes huge amounts of data from public institutions every day. The redundant connection with 10 gigabit lines speaks volumes for the data traffic. Some of this data is confidential or for internal use only and some of it is personal – such as citizens' financial data. The current regulations stipulate that such data may only be transported within the state's network with a strong encryption. However, the BSI goes one step further and requires a specific, deep encryption in accordance with advanced standards. So this is not just a challenge for Saarland; it is actually an opportunity to demonstrate its capacities in terms of IT security. The existing IPsec-based encryption is to be replaced by a modern, high-performance encryption, thus raising it to a new level. This will create the foundation for further secure digitalization in the federal state.

## The solution

In cooperation with hardware supplier Rohde & Schwarz Cybersecurity GmbH, the Saarland IT-DLZ developed a basic concept for the encryption solution. As the encryption and high-performance demands could not be met using software, the idea was to implement a high-performance hardware solution: the plan was to install an encryption box in each of the decentralized public administration sites and for the redundant clusters from

the encryption boxes to be integrated in the redundant 10 gigabit lines in the central data center. The boxes encrypt all data traffic on the layer 2 level. This concept had to be implemented on two separate occasions: once for the police and once for the IT-DLZ with its connected authorities. T-Systems came into play for the detailed planning of the concept and the actual rollout. T-Systems implemented the security measures. This not only included preparation and provision of support for the commissioning of the hardware boxes during the project, it also comprised the customization of them to meet the specific requirements of the state's data network and its authorities. After the original IPsec solution reached its performance limit, the layer 2 boxes in the data center provide a 40 gigabit encryption in the line speed which will also be able to cope with Saarland's increasing requirements in the medium-term. In addition to the general security management, T-Systems also designed and integrated features such as certificate management (users, devices) as well as the monitoring and logging of the new security platform. T-Systems is also responsible for the quick replacement of hardware and provision of support. 130 sites are currently being supported and an additional 75 sites will be added in the coming months. The solution is a highly-complex but equally flexible multipoint-to-multipoint layer 2 encryption. This means that not only the exchange of information between the sites and the central data center is secure; the sites can also communicate directly with each other with the highest security standards.

## Customer benefit

With the new multipoint-to-multipoint encryption, Saarland is the first federal state in Germany to have a modern layer 2 encryption solution that meets the strict BSI provisions for the transfer of VS-NfD documents. The site-to-site encryption effectively prevents exchanged documents, data streams, or emails from being intercepted by third parties. The concept is now considered a blueprint for use in other federal states. Also particularly noteworthy is the fact that the users do not notice any performance losses caused by the integration of hardware in these boxes. The central management server in the data center of the police and of the IT-DLZ creates the foundation to be able to independently manage and operate the solution. T-Systems provides support services 24/7 – malfunctioning boxes are also quickly replaced at the weekend in the event of an emergency. "With this solution, Saarland is not just consistently implementing "cybersecurity first". It is also providing a template for Germany, showing how complete encryption of all the state's authorities can be implemented across the board," summarizes Ammar Alkassar, Authorized Representative for Innovation and Strategy and Saarland CIO. With the comprehensive encryption, Saarland has laid the foundation to implement its digital vision.

### Further advantages:

- Positioning as a pioneer for IT security in the public sector
- Basis for the implementation of digital plans
- Future-oriented, high-performance security solution
- Customized by T-Systems
- 24/7 support services

### Contact

T-Systems International GmbH  
Hahnstraße 43d  
60528 Frankfurt am Main, Germany  
E-Mail: [referenzen@t-systems.com](mailto:referenzen@t-systems.com)  
Internet: [www.t-systems.com](http://www.t-systems.com)

### Published by

T-Systems International GmbH  
Marketing  
Hahnstraße 43d  
60528 Frankfurt am Main  
Germany