Federal Ministry
Transport, Innovation
and Technology

KIRAS
Security Research

Bontempiorgel

Martin LATZENHOFER

e 2 0
u 1 8
· a t

Bundesministerium
Verkehr, Innovation
und Technologie

Bontempiorgel

Behoerdennetzwerk – Implementierungsvorschlag für eine Staatsgrundnetzlösung

Public Authorities‘ Network – Implementation Proposal for a Governmental Network Solution

Martin Latzenhofer, Ivan Gojmerac, Alessandro D'Alconzo, Florian Skopik, Maria Leitner
Austrian Institute of Technology, Center for Digital Safety & Security

Austro-European Security Research Innovation Days
June 25th, 2018

KIRAS
Security Research

AGENDA

- Why is it necessary?
- What is the project outline?
- Who needs an authorities' network?
- What are the architectural key aspects?
- What are the key results?

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Federal Chancellery

Federal Ministry
Interior

BMLV
BUNDESMINISTERIUM
FÜR LANDESVERTEIDIGUNG

THE CURRENT SITUATION

- Society‘s dependency on technology is enormous now
- Interdependencies of critical infrastructures are evident
- Cost pressure on federal authorities forces the adoption of private structures
- Outsourcing of ICT services is very common, even in governmental environments
  - Hand over of costs, employees, risk; but also control, design flexibility, know-how
  - Service responsibility still remains with the government
  - Service providers have different organizational strategies and objectives
  - Growing international economic interrelation and ownership structures limit the scope of action
- The government needs to ensure **functional operability with its own measures** even in case of a severe incident affecting critical infrastructures.

→ **What happens if something happens?**

THE FORMAL PROJECT OUTLINE

- KIRAS call February 2016
- Public clients
  - Federal Ministry for the Interior (BM.I), Department I/11, Office for Security Policy,
    MR Kurt Hager, BA MA
  - Federal Chancellery of Austria (BKA), Department IV/6, Security Policy and National Security Council
    Dr. Helmut Schnitzer
  - Federal Ministry for Defence (BMLVS)
    MR Hannes Baumgartner, BA MA MSc
- The project is information classified “restricted”
- Research study was finished in November 2017
- Research and development services, net cost were 99k EUR


AUSTRIAN INSTITUTE OF TECHNOLOGY

Studie im Rahmen des
KIRAS Forschungsprogrammes

Behördennetzwerk–
Implementierungsvorschlag
für eine Staatsgrundnetzlösung

Alessandro D'Alconzo
Ivan Gojmerac
Martin Latzenhofer
Maria Leitner
Stefan Schauer
Florian Skopik
Martin Stierle

Informationsklassifizierung nach Informationssicherheitsverordnung (InfoSiV):

EINGESCHRÄNKT (E)

30.11.2017

Exemplar 1

FFG-Projektnummer: 854745 – Projektkurzname „Bontempiorgel"

THE CONTENT OF THE PROJECT

- An authorities' network ensures the **availability and security of communication** between key stakeholders in case of a major safety or security crisis.
- It **overcomes existing dependencies** of authorities on external private information and communication (ICT) service providers, the **heterogeneity** of the current network architecture and **uses unexploited technical potential** of different ICT networks of public authorities.
- The project outlines a **requirements specification** for the implementation of a public authorities' network with special focus on the **reuse** of existing infrastructure.

→ **The project's result is a research study that can serve as a discussion basis for a political and strategic decision on the implementation of a public authorities' network.**

A POSSIBLE SOLUTION

- An authorities' network shall ensure that at least public authorities (national, regional and local) and critical infrastructure providers are able to cope with an ICT breakdown in order to ensure the operative functionality of the government in a exceptional situation…
  - with technically reasonable effort,
  - with preferably own and already existing measures and structures,
  - with focus on collaboration, communication and information exchange by a loosely connected network in cooperation with all federal organisations,
  - providing a secure environment, which is reliable, 24x7 available, simple to operable, smoothly and seamlessly linked without requiring an explicit activation by users.

→ **Establishing an authorities' network is a prerequisite for resilience in a situation of cascading effects due to simultaneous failures of several critical infrastructures.**

THE PARTICIPANTS

Ministries with responsibility for national security

- The clients of this project and responsible organisations for national security of this project BKA, BM.I and BMLV are the core stakeholders of this project due to their political responsibility.

National, regional, local authorities including district administration and communities

- The administrative organisations benefit from support and clear leadership skills of the crisis team.

First responder, blue-light organisations

- The leaders of the first responders in situational awareness centres communicate local situations contributing to a comprehensive perspective.

Critical infrastructure providers

- Around 400 providers of critical infrastructure services can be an optional part of an authorities' network according to the type of crisis and/or affected infrastructures.

ICT network providers

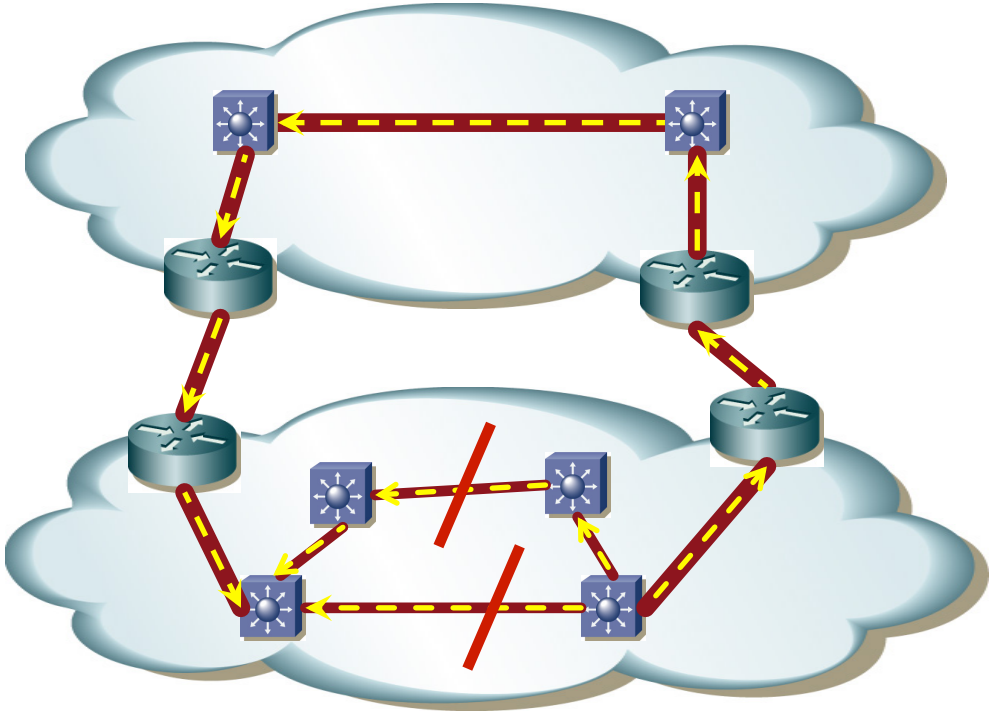
- They benefit from increased reliability, security of their own network.

→ The circle of participants is not closed, unidirectional communication should be possible.

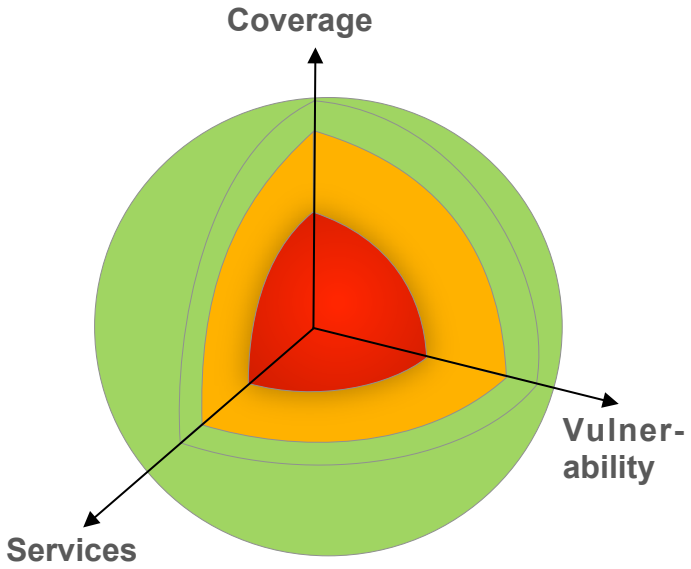
THE ARCHITECTURAL CONCEPT: NETWORK PARTITIONING

- Application scenario is based on network partitioning
- Use of existing different federal network structures
- Applying tunnelling technologies as automatic failover

→ **An explicit failover switch is not necessary due to intelligent network configuration.**



THE ARCHITECTURAL CONCEPT: ONION STRUCTURE



Intelligent Network Interconnection

Automatic failover configuration by applying tunneling technologies and prioritizing services.

Dedicated Authorities‘ IP Network

Restricted number of dedicated endpoints with higher reliability.

Reliable Core Technologies

Only core services carried via foreign legacy networks.

Services and their Relative Priorities from the Authorities‘ Perspective

1. Voice Communication
2. Written Communication (Email)
3. Command & Control
4. Video Communication
5. Data Exchange

THE ARCHITECTURAL CONCEPT: OPERATION MODES I

① **Normal Operation, Tasks and Objectives**

- Identification of the critical network infrastructure which should be protected based on available infrastructures of all participants
- Determination of the best technical solution based on the technology of available systems, configuration and maintenance cost of the failover infrastructure
- Arrangement of bilateral/multilateral Service Level Agreements (SLA) with other participants of the authorities' network (access and usage of the host infrastructure)
- Design, configuration and implementation of traffic tunnels, which will be activated in Mode 2
- Testing of the failover infrastructure

→ **All communication channels are functioning normally.**

② **Simple Crisis**

- Only a single critical infrastructure is affected → failover Layer 1

→ **The same systems are still in operation, but the communication is prioritized.**

THE ARCHITECTURAL CONCEPT: OPERATION MODES II

③

Complex Crisis

- Several critical infrastructures are affected → failover Layer 1 or 2

→ **There is exclusive communication on independent lines and devices even when other normal operating networks fail.**

④

Overwhelming Crisis

- Stand-alone communication based on restrictive governance
- Typical examples: long lasting power outage, large-scale or nuclear catastrophe, etc.
- Failover switching to the core components of the authorities' network

→ **If there are no available networks anymore (due to large-scale failures) stand-alone networks that are not under responsibility of the government should be used as communication medium.**

KEY FINDINGS

- It is necessary to cope with the growing complexity of communication.
- Synergy effects between existing network structures should be used.
- Communication is a key aspect for resilience, coordination, and cooperation of authorities.
- Information security will be further improved by an authorities' network.
- Need for a secured communication environment for blue-light organisations, ministries, critical infrastructure providers, and decision-makers at the federal, regional and local level.
- Services should be categorized and prioritized.
- Focus on a modular technical architecture to support financial, technical and economic considerations.
- Implementation, operation and activation of the authorities' network requires clear political, legal and organisational rules for governance on the tactical level.
- This new critical infrastructure requires a comprehensive risk analysis.

→ **The study serves as a basis for a political and strategic decision whether Austria should develop and invest in an innovative authorities' network solution.**

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Martin Latzenhofer

June 25th, 2018