



Realtime Security
for Enterprise Networks
based upon the
Correlation of Metadata

Josef von Helden

(University of Applied Sciences and Arts, Hanover)

15.06.2011, München

Introduction



Trust@FHH Research Group

- Team
 - Chair: Prof Dr. Josef von Helden
 - 3 research associates
 - 4 student assistants
- Research Fields
 - Trusted Computing
 - Network & Mobile Security
- Selected Projects
 - TNC@FHH
 - IRON
 - ESUKOM
- More Information
 - trust.inform.fh-hannover.de



ESUKOM overview



The ESUKOM Project in a Nutshell

- Motivation
 - Smartphones are used in business environments
 - Impact of Smartphones in terms of IT-Security is unclear
 - Idea: Address **Smartphone Challenge** by leveraging IF-MAP
- Project Goals
 - Investigation of Smartphone platforms in terms of security
 - Development of IF-MAP prototype infrastructure
- Duration
 - 10/2010 – 09/2012 (2 years)
- Funding
 - Funded by german BMBF
- Website
 - www.esukom.de

SPONSORED BY THE



Federal Ministry
of Education
and Research



Project Consortium

- 3 SMEs & 2 Academic Institutions

- DECOIT GmbH
- mikado soft GmbH
- NCP engineering GmbH
- Fraunhofer SIT
- Trust@FHH, FH Hannover

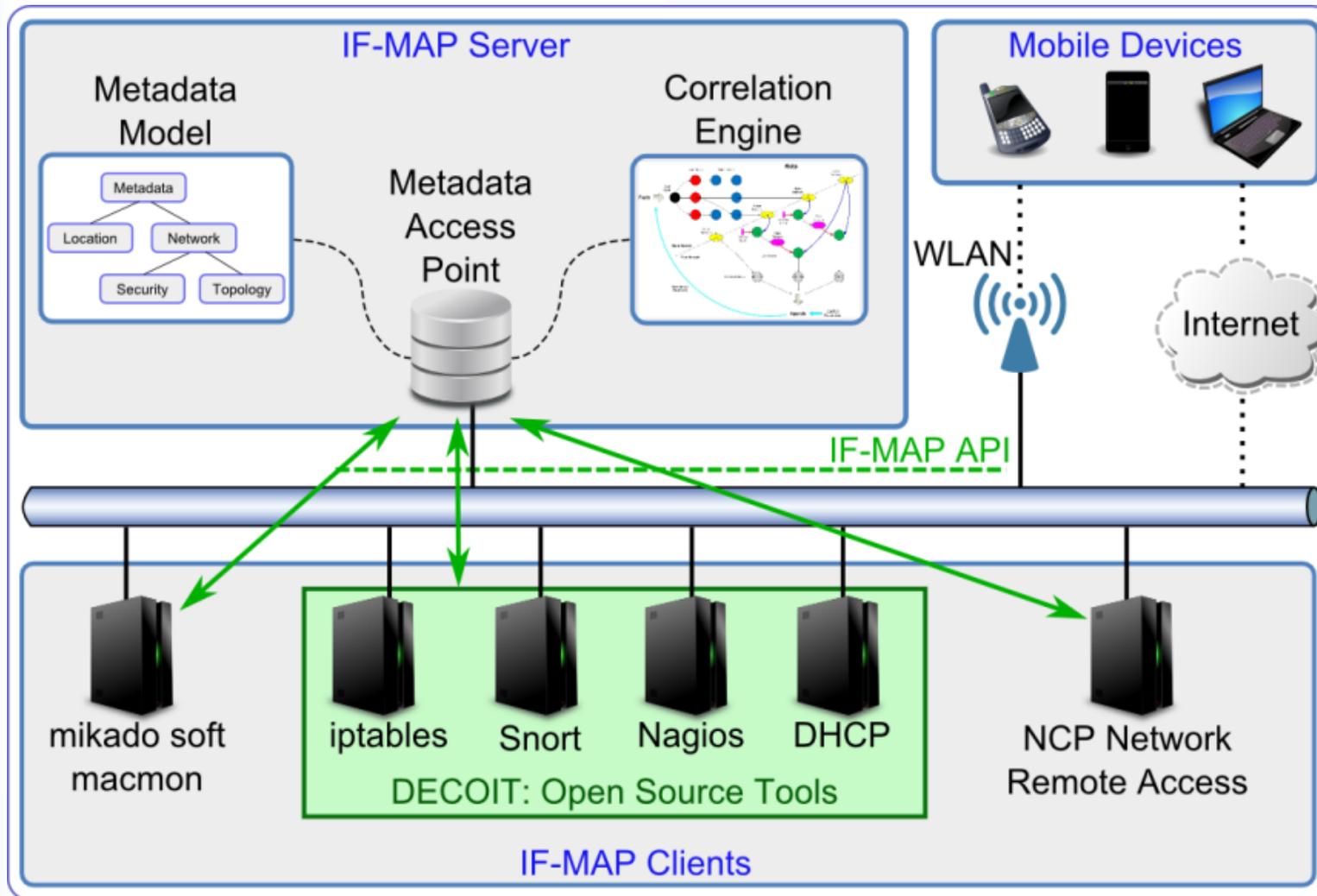


- Further Cooperations

- Infoblox, Juniper, Enterasys, Infineon
- PhD Programme with Universität der Bundeswehr München



ESUKOM High Level Architecture



Mobile Phone Security



Smartphone Threat Analysis for ESUKOM

- Goal
 - Threat model for smartphones used in corporate environments
 - Smartphones == mobile consumer electronic devices
- Smartphone Characteristics
 - Built-in Sensors
 - Connectivity
 - Internet-support
 - Resource Paradox
 - App-based Architectures
 - Platform Diversity



Smartphone Threat Analysis for ESUKOM

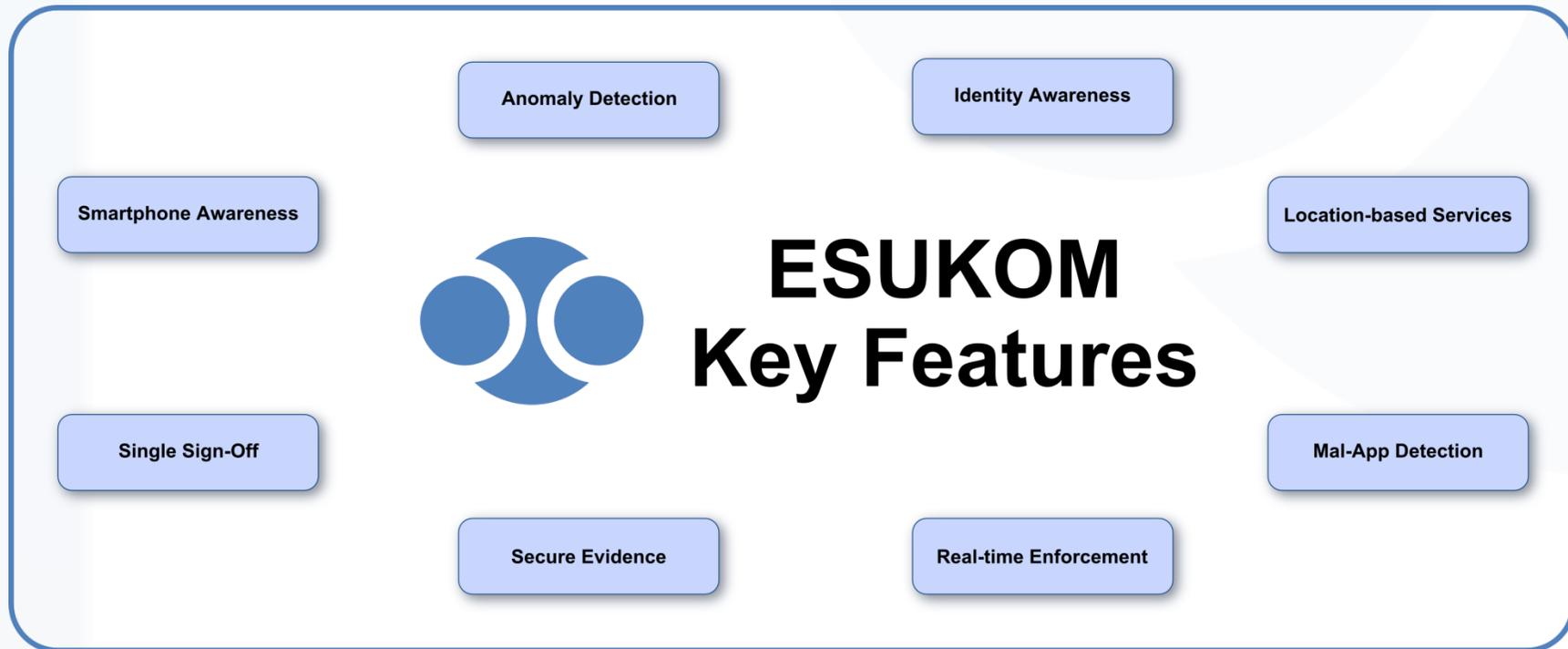
Target of Attack	Physical Environment	Smartphone	IT-Infrastructure
Exemplary Attacks	<ul style="list-style-type: none">Sensory Mal-AppsInsider Sensor Sniffing	<ul style="list-style-type: none">Resource Exhaustion Mal-AppsTrojan SMS/MMS SpammingLocal Data Sniffing Mal-AppsBotnet Mal-AppsPhysical Loss / Theft	<ul style="list-style-type: none">Smartphone Mounted Data TheftSmartphone Mounted Profiling



ESUKOM Key Features



ESUKOM Key Features



ESUKOM Development



ESUKOM Development: Overall Planning

	Anomaly Detection	Smartphone Awareness	Identity Awareness	Location-based Services	Mal-App Detection	Real-time Enforcement	Secure Evidence	Single Sign-Off	Responsibility
macmon	P/S	P	P	P/S	S	S	P		MIC
NCP VPN	P/S	P	P	P	S	S			NCP
(Free) RADIUS	P		P				P	P/S	DEC
Snort	P				P/S	P			DEC
Detection Engine	P/S	S		P/S	P/S	P/S			FHH
Nagios	P								DEC
iptables			P/S	P/S		S			DEC
Smartphone	P/S	P	P	P	P/S		P/S		FHH
DHCP			P				P		FHH
IRONGUI	S	S	S	S	S	S	S	S	FHH
Timing Authority							P		SIT
TNC Server							P/S		SIT
Privacy CA							P		SIT
Evidence DB							S		SIT
Open VPN (Redundancy to NCP VPN)	P/S							P/S	DEC

P = Publish	S = Subscribe	P/S = Publish + Subscribe
-------------	---------------	---------------------------



ESUKOM Development

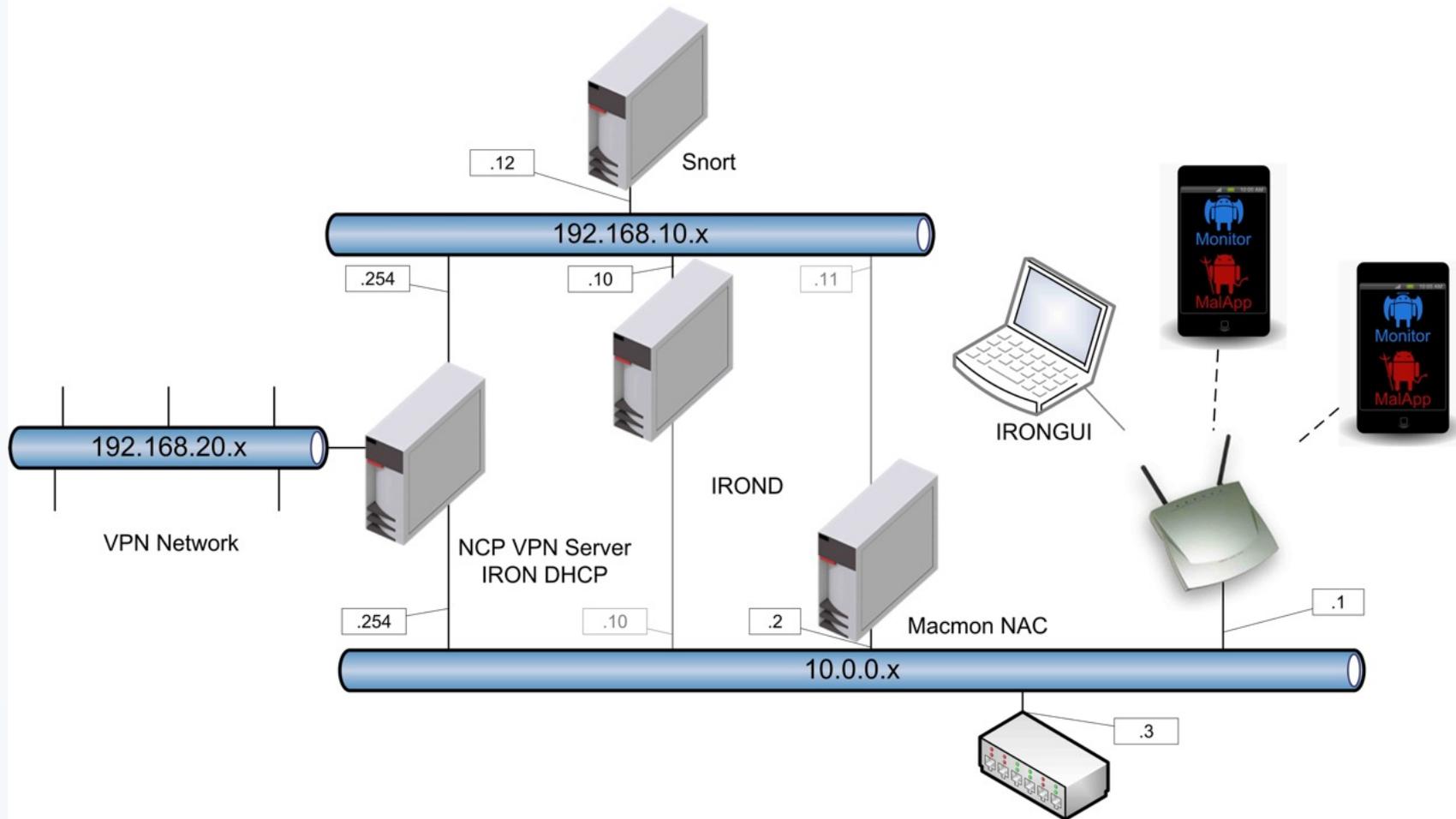
- Status by 15/06/2011
 - Publish functionality of standard metadata by MAP Clients
 - NCP VPN Gateway
 - mikado soft macmon
 - Snort
 - Android Smartphone
 - DHCP
 - MAP Server
 - ironD
 - Visualization
 - ironGUI
 - subscribe / search functionalities: under development



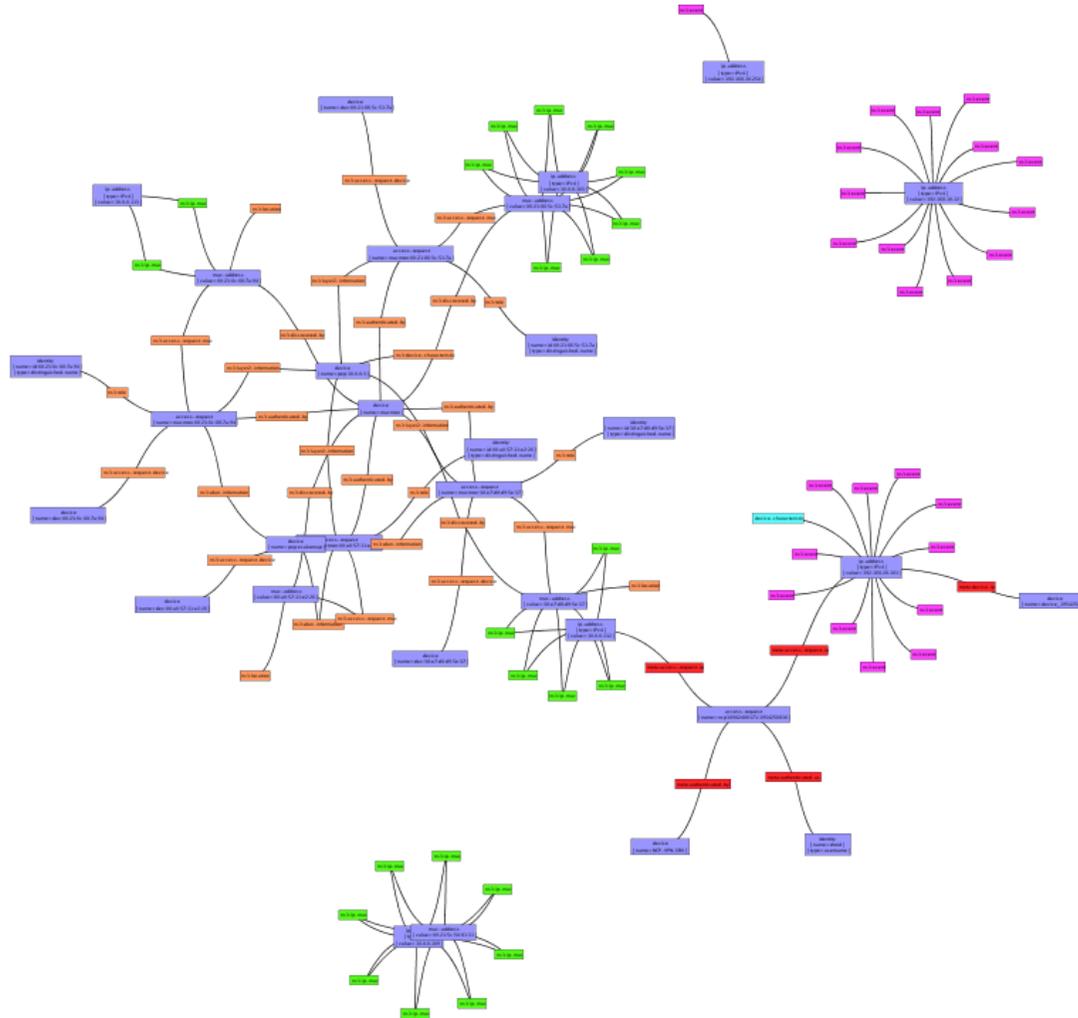
Live Demo



ESUKOM Demo Setup



ESUKOM Demo: Screenshot irongui



Open (Research) Questions



Open (Research) Questions

- Effective correlation of large metadata graphs
 - What are suitable correlation approaches?
 - What part of metadata graph is relevant for what purpose?
- Trustworthiness of metadata graph

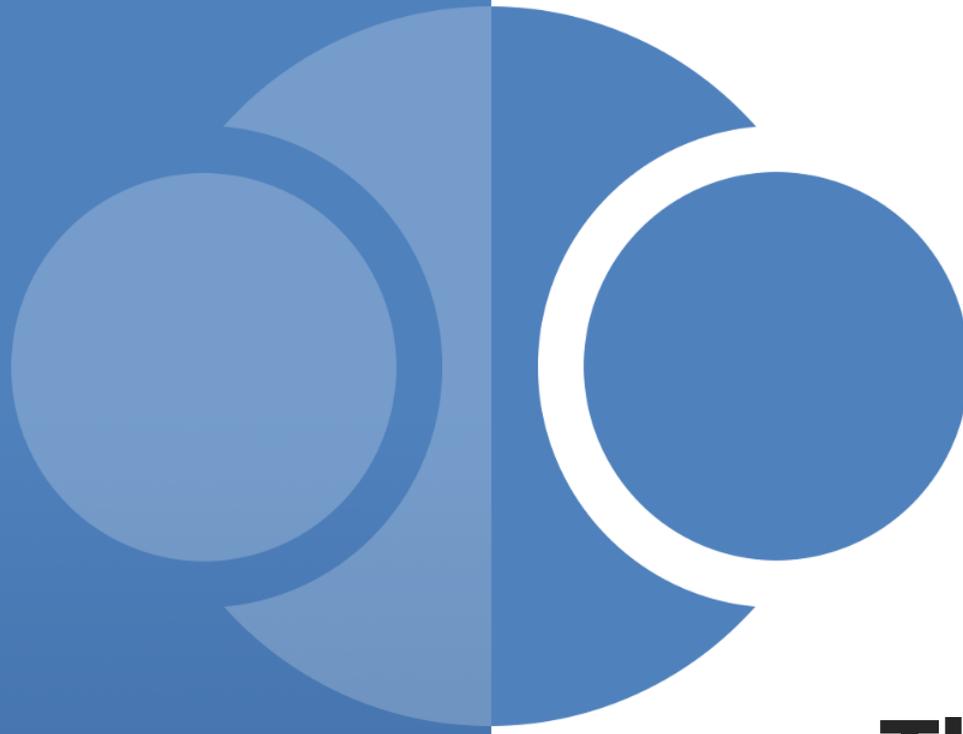
=> Detection Engine



Further Open (Research) Questions

- Smartphone specific metadata vocabularies
 - Status of sensors
 - Platform configuration (installed apps, used permissions)
- Interdomain MAP
 - MAP-Server to MAP-Server Communication
- Threats introduced by IF-MAP?
 - Impact of rogue MAPCs





Thank You
Questions ?

Copyright 2011

Das dem Projekt zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen „01BY1050“ gefördert. Die Verantwortung für den Inhalt liegt bei den Autoren.

*Die in dieser Publikation enthaltenen Informationen stehen im Eigentum der folgenden Projektpartner des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projektes „**ESUKOM**“: DECOIT GmbH, Fachhochschule Hannover (FHH), Fraunhofer-Institut für Sichere Informationstechnologie (SIT), NCP engineering GmbH und der mikado soft GmbH. Für in diesem Dokument enthaltenen Information wird keine Garantie oder Gewährleistung dafür übernommen, dass die Informationen für einen bestimmten Zweck geeignet sind. Die genannten Projektpartner übernehmen keinerlei Haftung für Schäden jedweder Art, dies beinhaltet, ist jedoch nicht begrenzt auf direkte, indirekte, konkrete oder Folgeschäden, die aus dem Gebrauch dieser Materialien entstehen können und soweit dies nach anwendbarem Recht möglich ist.*

