Tobias Guggemos, Nils gentschen Felde, Dieter Kranzlmüller
MNM-Team
Ludwig-Maximilians-Universität München

Secure Group Communication in Constrained Networks – A Gap Analysis

IEEE Global IoT Summit 2017
Geneva, Switzerland

Motivation

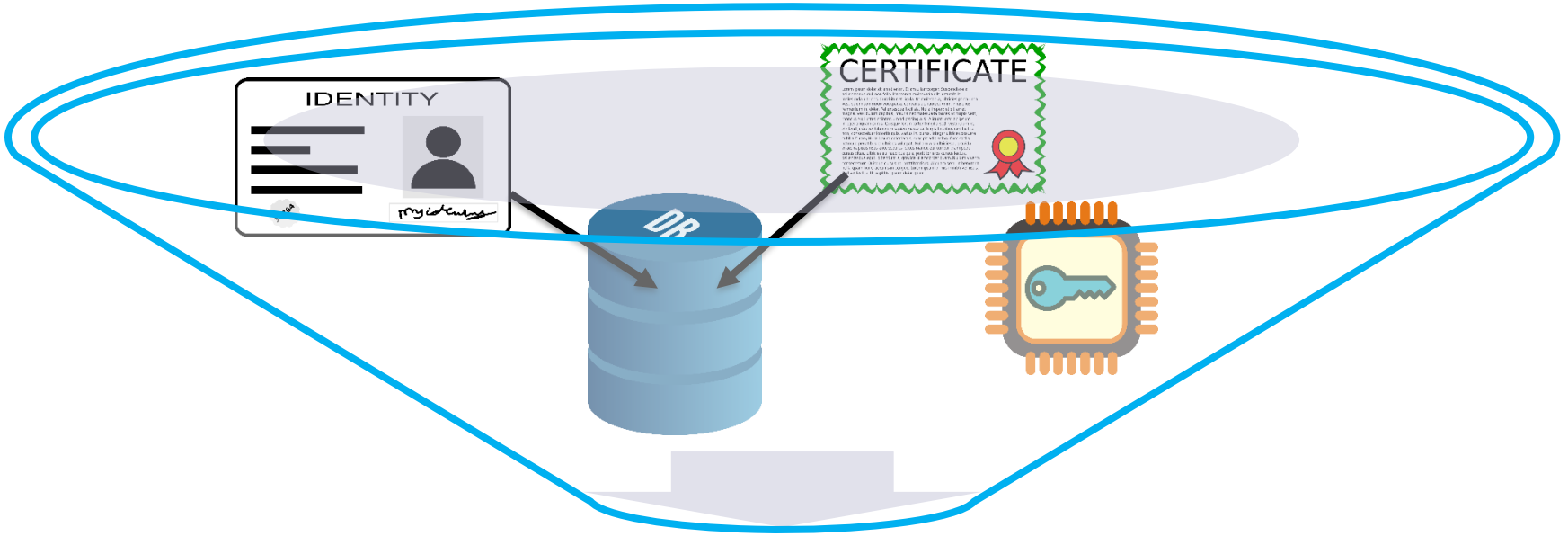
Since ~2013:

Several and long discussions about

Secure Group Communication

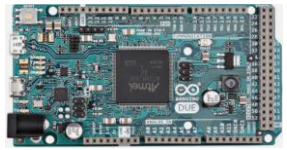
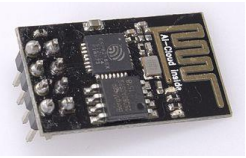
in IETF working groups (DICE, ACE, …)

The Goal

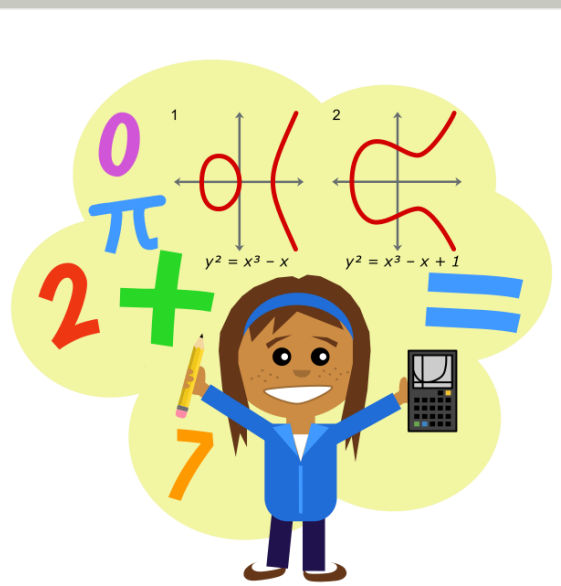


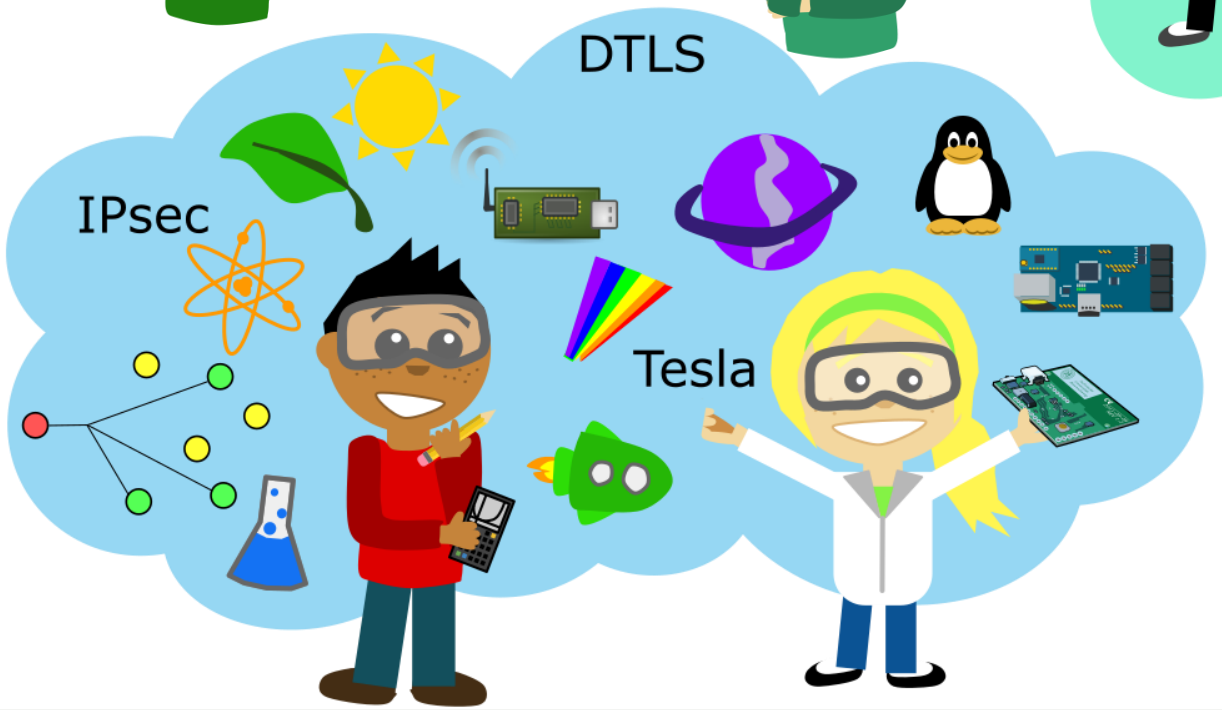
Toolbox for Secure Group Communication in constrained environments (e.g. IoT)

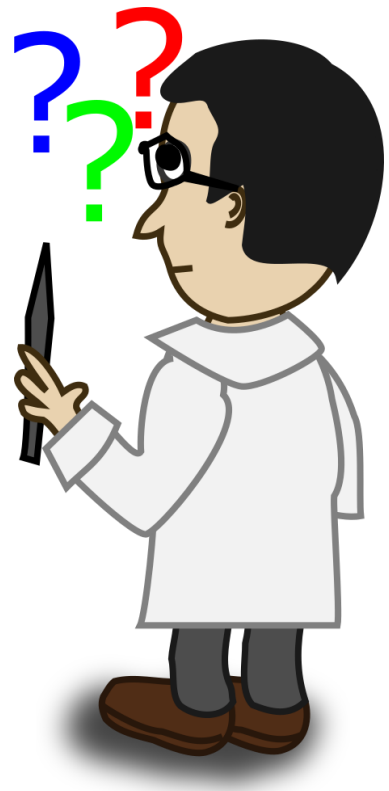
Motivation - Testbed

Devices	 Arduino Uno	 Arduino M0+	 Arduino Due	 ESP 8266	 Raspberry Pi (v1-v3) Banana Pi Beaglebone
Architecture	ATmega328	ARM Cortex-M0+	ARM Cortex-M3	Tensilica L106	ARMv6 – ARMv8
CPU	16 MHz	48 MHz	84 MHz	80-160 MHz	700-1200 MHz
RAM	2 KB	32 KB	96 KB	64 KB	256-1024 MB
Flash	32 KB	256 KB	512 KB	1 MB	
Operating System	RIOT OS	RIOT OS	RIOT OS	Free RTOS	Linux

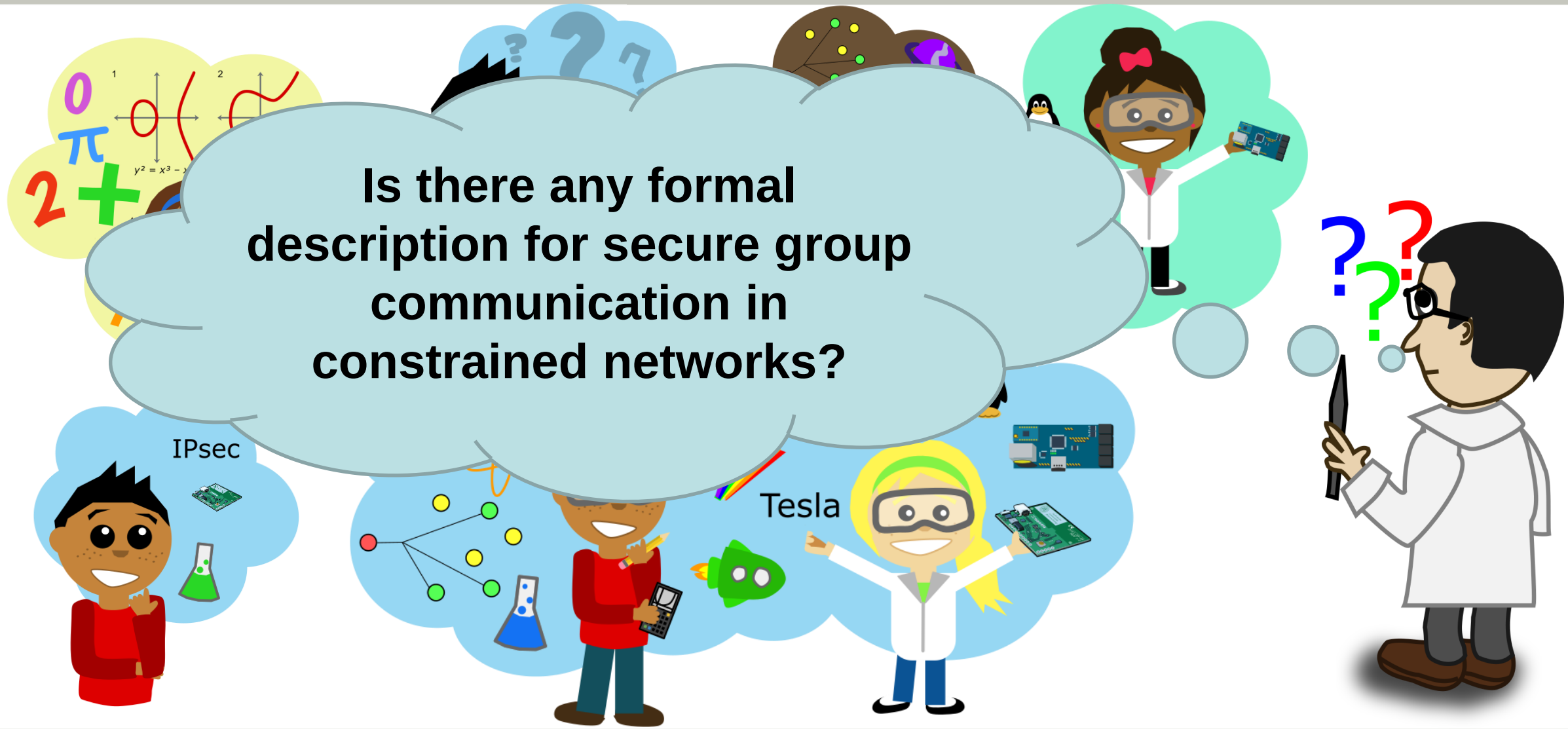
Motivation



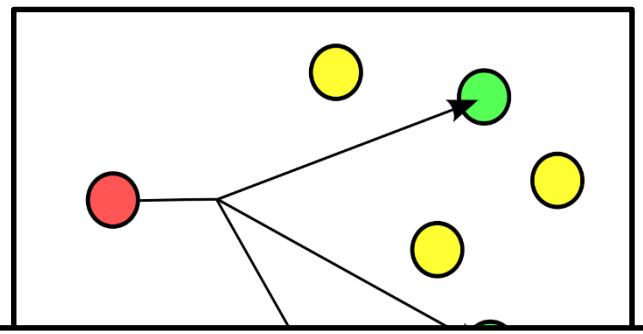


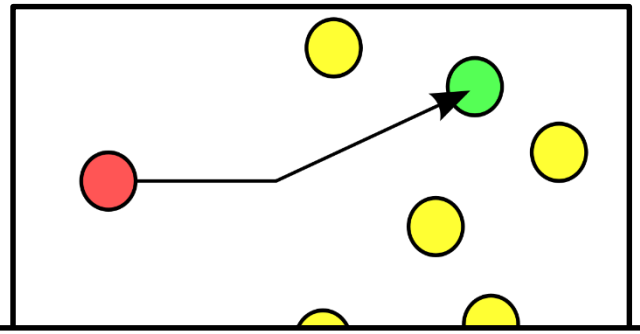


Motivation


Is there any formal description for secure group communication in constrained networks?
IPsec
Tesla

What is *Group* Communication?





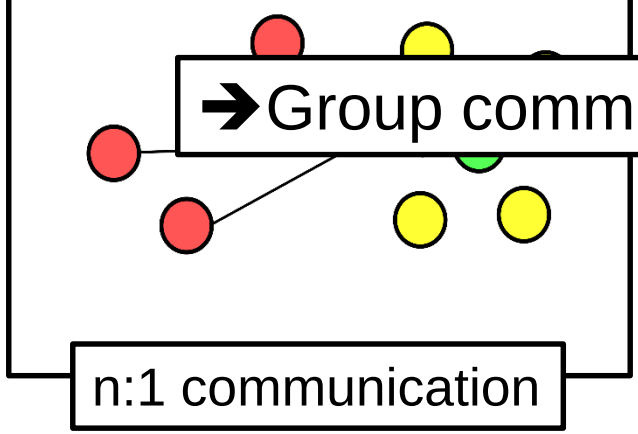
➔Group communication includes most major IoT-related communication models

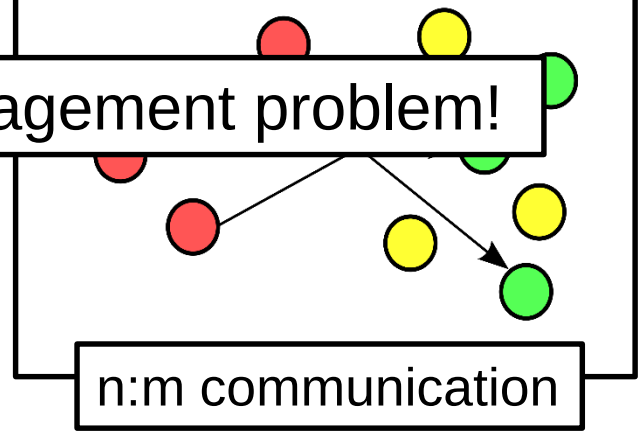
1:n communication

1:1 communication

➔Securing groups can help securing IoT in general

➔Group communication is a management problem!





n:1 communication

n:m communication

Question

What is
"Secure Group Communication"

What is
"Secure Group Management"

What is secure?

Definition according to ISO/IEC 27000:

"**information security**

preservation of **confidentiality** (2.13), **integrity** (2.36) and **availability** (2.10) of information

NOTE In addition, other properties, such as **authenticity** (2.9), **accountability** (2.2), **non-repudiation** (2.49), and **reliability** (2.56) can also be involved."

[ISO/IEC27000, 2.30]

What does that mean for Group Communication?

Definition accordin[illegible]27000:

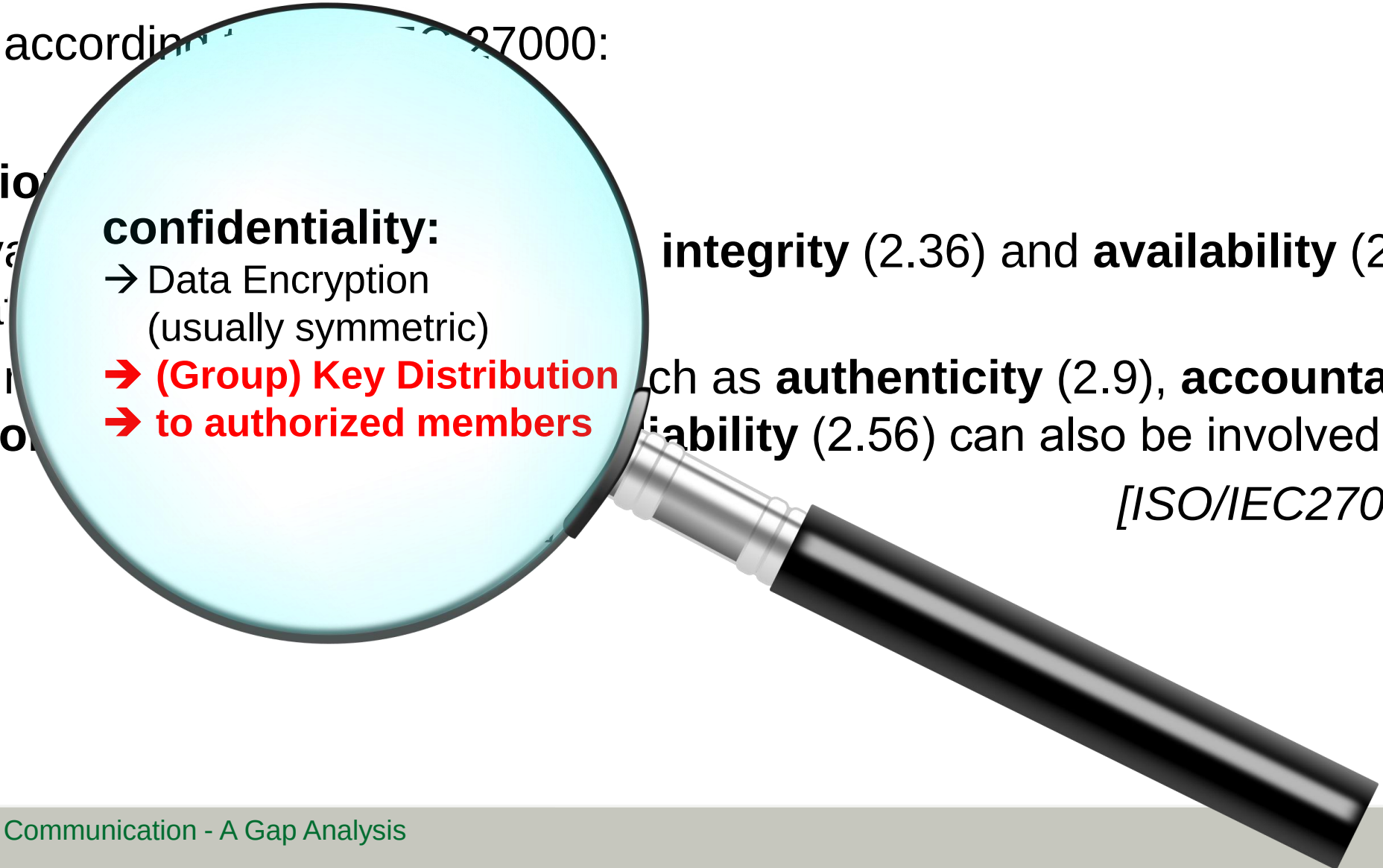
"**informatio**[illegible]

preserva[illegible] **integrity** (2.36) and **availability** (2.10) of informa[illegible]

NOTE I[illegible]ch as **authenticity** (2.9), **accountability** (2.2), **no**[illegible]**iability** (2.56) can also be involved."

[ISO/IEC27000, 2.30]

confidentiality:
→ Data Encryption
(usually symmetric)
➔ **(Group) Key Distribution**
➔ **to authorized members**



What does that mean for Group Communication?

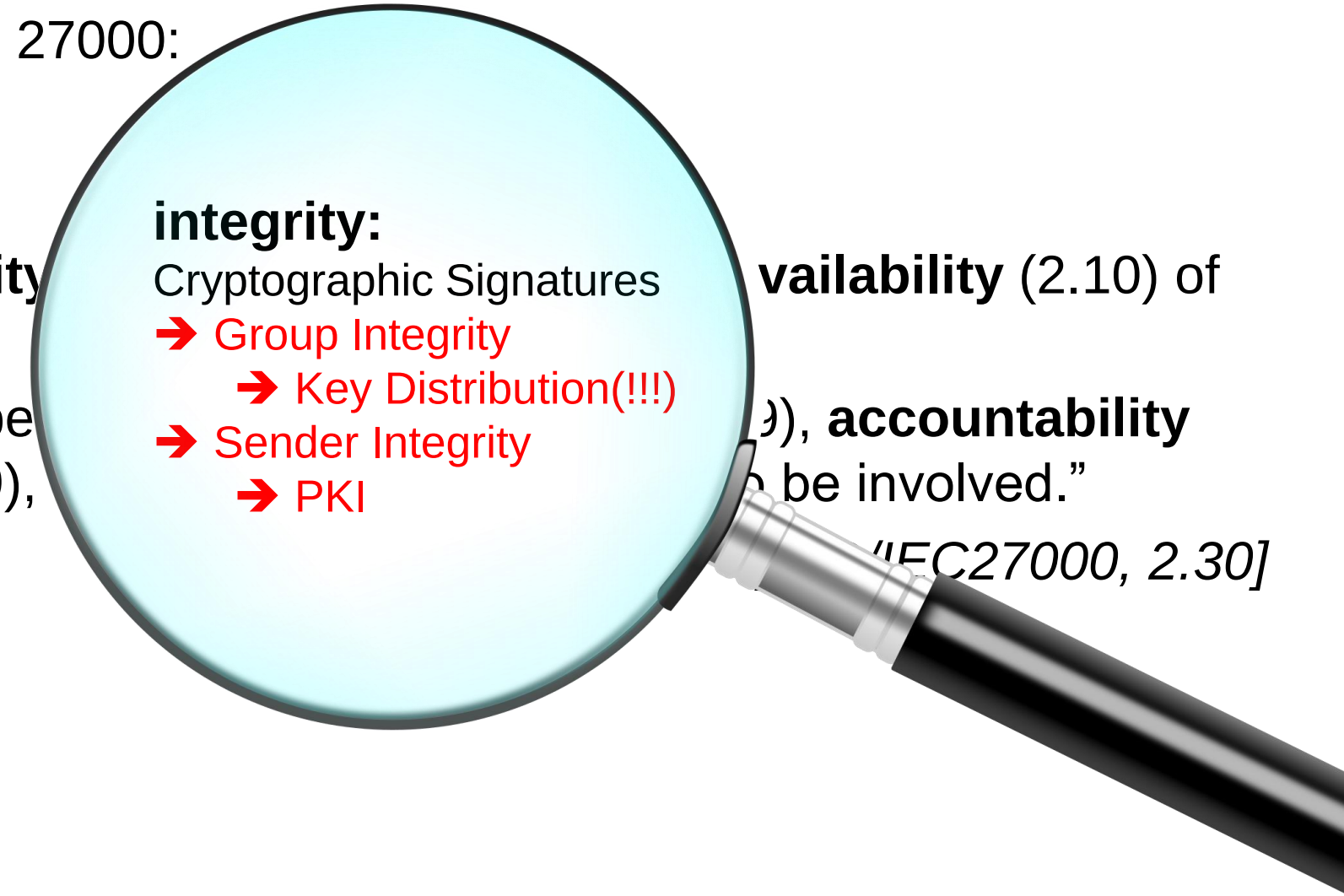
Definition according to ISO/IEC 27000:

"**information security**

preservation of **confidentiality** … **vailability** (2.10) of information

NOTE In addition, other prope… …), **accountability** (2.2), **non-repudiation** (2.49), … be involved."

[ISO/IEC27000, 2.30]



What does that mean for Group Communication?

Definition according to ISO/IEC 27000:

"**information security**

preservation of **confidentiality** (2.13), **integrity** of information

NOTE In addition, other properties, such as **aut** (2.2), **non-repudiation** (2.49), and **reliability** (2.

What does that mean for Group Communication?

Definition according to ISO/IEC 27000:

"**information security**

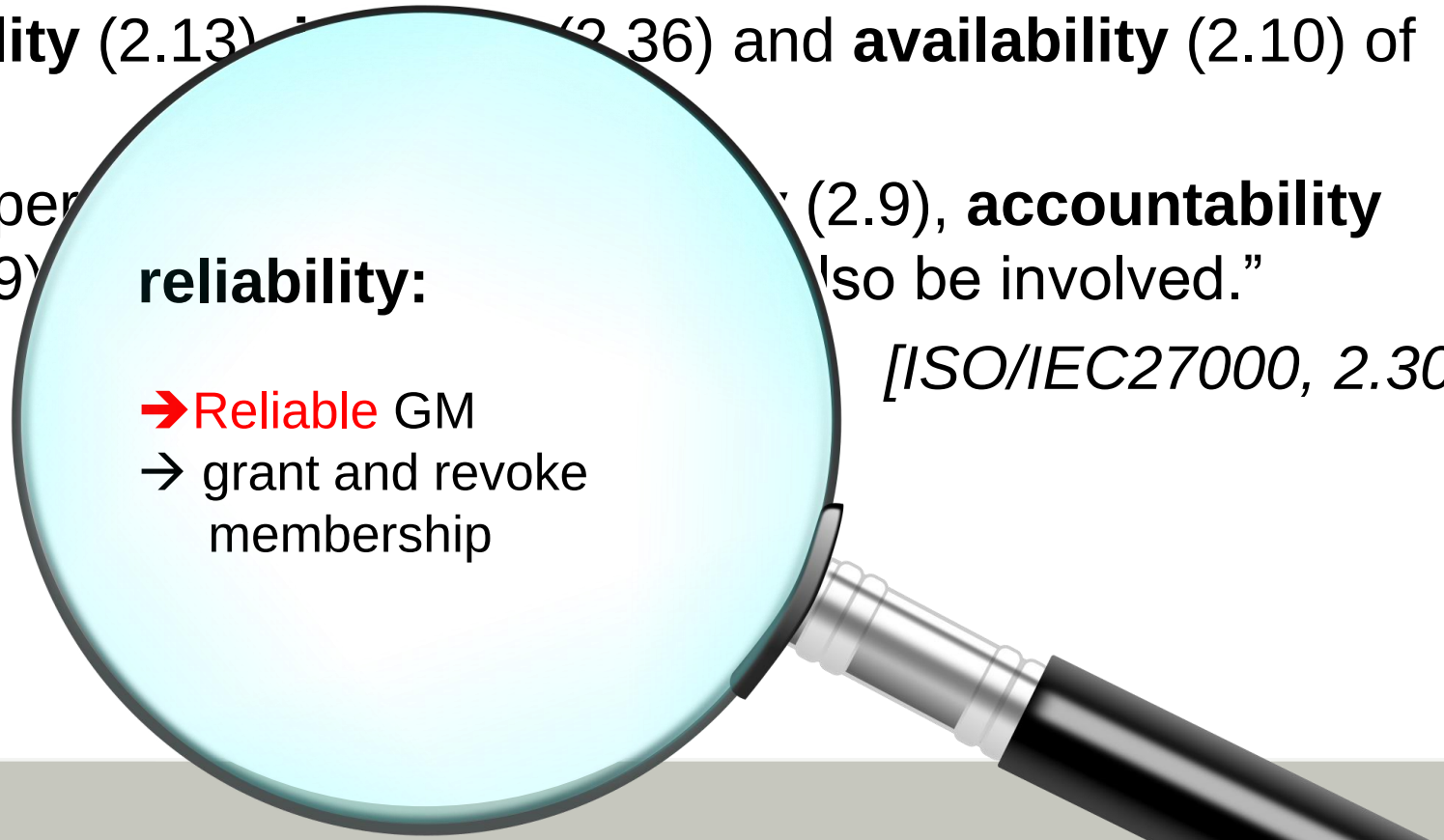
preservation of **confidentiality** (2.13), **integrity** (2.36) and **availability** (2.10) of information

NOTE In addition, other properties, such as **authenticity** (2.9), **accountability** (2.2), **non-repudiation** (2.49) and **reliability** can also be involved."

[ISO/IEC27000, 2.30]

reliability:

➔Reliable GM
→ grant and revoke membership



What does that mean for Group Communication?

Definition according to ISO/IEC 27000:

"**information security**

preservation of **confidentiality** (2.13), **integrity** (2.36) and **a**[illegible] **f** information

NOTE In addition, other properties, such as **authenticit**[illegible] (2.2), **non-repudiation** (2.49), and **reliability** (2.56) ca[illegible]

accountability:

➔Right Management
- → join, leave,
- → create,destroy
- → send messages

What does that mean for Group Communication?

Definition according to ISO/IEC 27000:

"**information security**

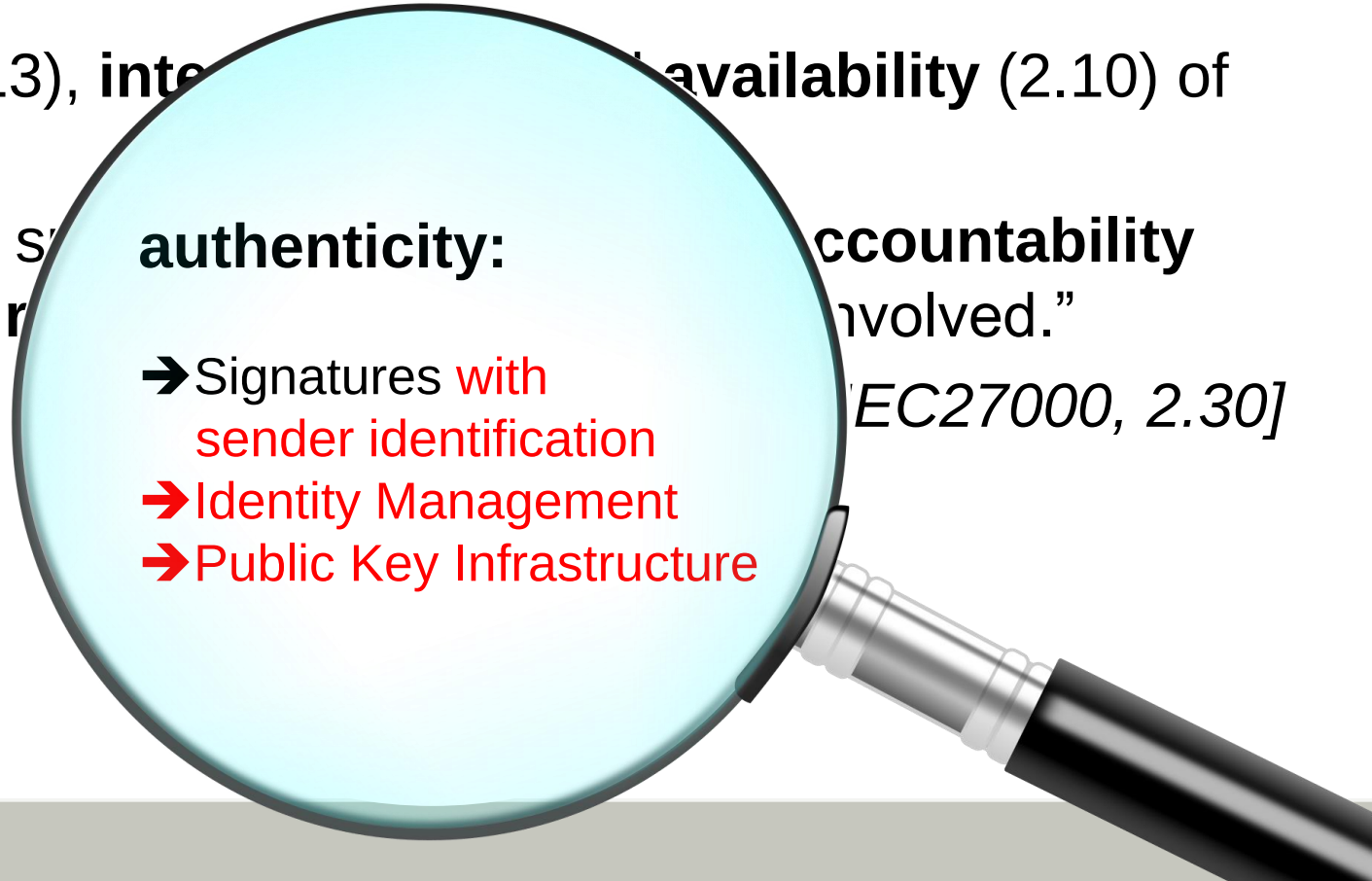
preservation of **confidentiality** (2.13), **inte** **availability** (2.10) of information

NOTE In addition, other properties, s **ccountability** (2.2), **non-repudiation** (2.49), and **r** nvolved."

EC27000, 2.30]

authenticity:

➔Signatures with sender identification
➔Identity Management
➔Public Key Infrastructure



What does that mean for Group Communication?

Definition according to ISO/IEC 27000:

"**information security**

preservation of **confidentiality** (2.13), **integrity** (2.36) and **availability** (2.10) of information;

NOTE In addition, other properties, such as **authenticity** (2.9), **accountability** (2.30), **non-repudiation** (2.44) and **reliability** (2.56) can also be involved."

[ISO/IEC27000, 2.30]

non-repudiation:

➔ Sender Authentication
AND Identity
AND Public Key Management
➔ Message ID (Seq. Nr)
➔ Acknowledgement (?)

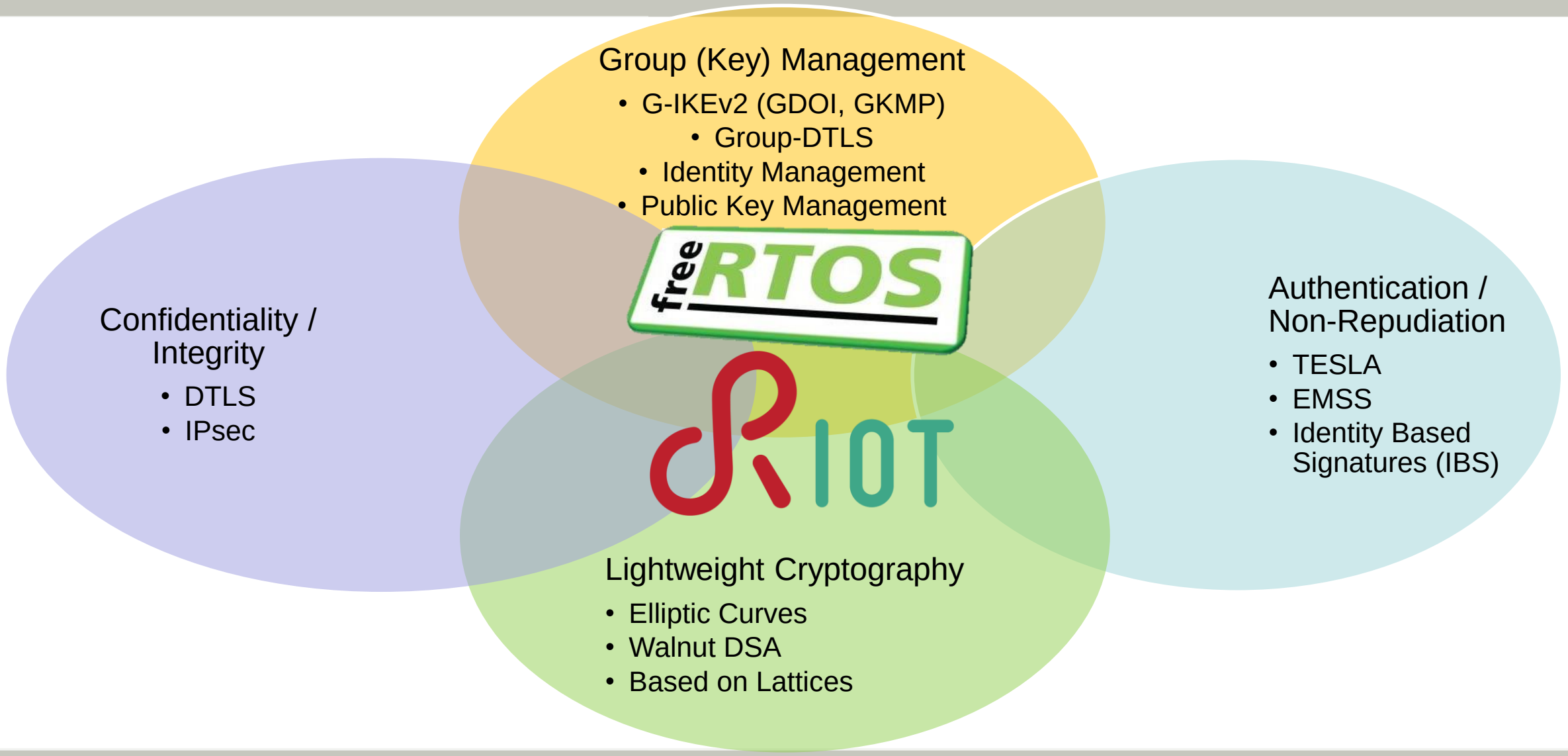
Gap Analysis

Related Work	Confidentiality	Integrity	Availability	Authenticity	Accountability	Non-Repudiation	Reliability
III-A: Group CoAP (RFC 7390)	✘	✘	(✔)[a]	✘	✘	✘	✔
III-A: DICE (RFC 7925)	✘	✘	(✔)[a]	✘	✘	✘	✔
III-A: Group DTLS [3]	✔	(✔)[b]	✔	(✔)[b]	✔	✘[b]	✔
III-B: IPsec	✔	(✔)[b]	(✔)[a]	(✔)[b]	✘	✘[b]	✔
III-B: Group-DH [4]	✘	✘	✔	✘	✔	✘	✔
III-C: EMSS [5]	✘	(✔)[d]	✘[c]	(✔)[d]	✘	✔	✘[c]
III-C: TESLA [5]	✘	✔	✔	✔	✔	✘	✔
III-C: μTESLA [6]	✘	(✔)[b]	✔	(✔)[b]	✔	✘	✔
III-C: IBS [7]	✘	✔	✘[c]	✔	✘	✘[e]	✘
III-C: ABE [8]	✔	✘	✘	✘	✘	✘	✘

legend: ✔ addressed by design (✔) partially addressed ✘ not addressed by design

[a] unauthenticated group management [b] no message source authentication/integrity. [c] no group management [d] delayed signature verification
[e] no anti-replay mechanism

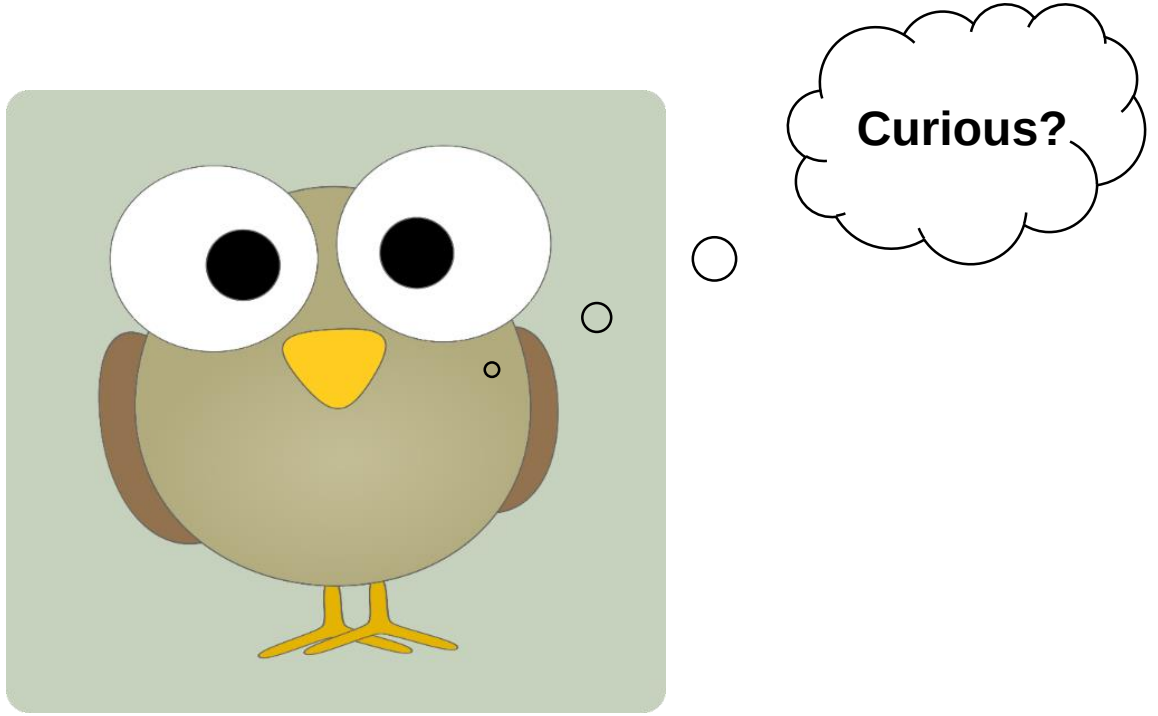
Current & Further Investigations



Conclusion / Take Aways

- Secure Group Communication is a management problem
- We defined properties for Secure Group Management
- Analysis shows no existing „IoT-aware“ solution
- Research requires a solid testbed:
  → MNM-Team setup: www.mnm-team.org/projects/embedded

The End



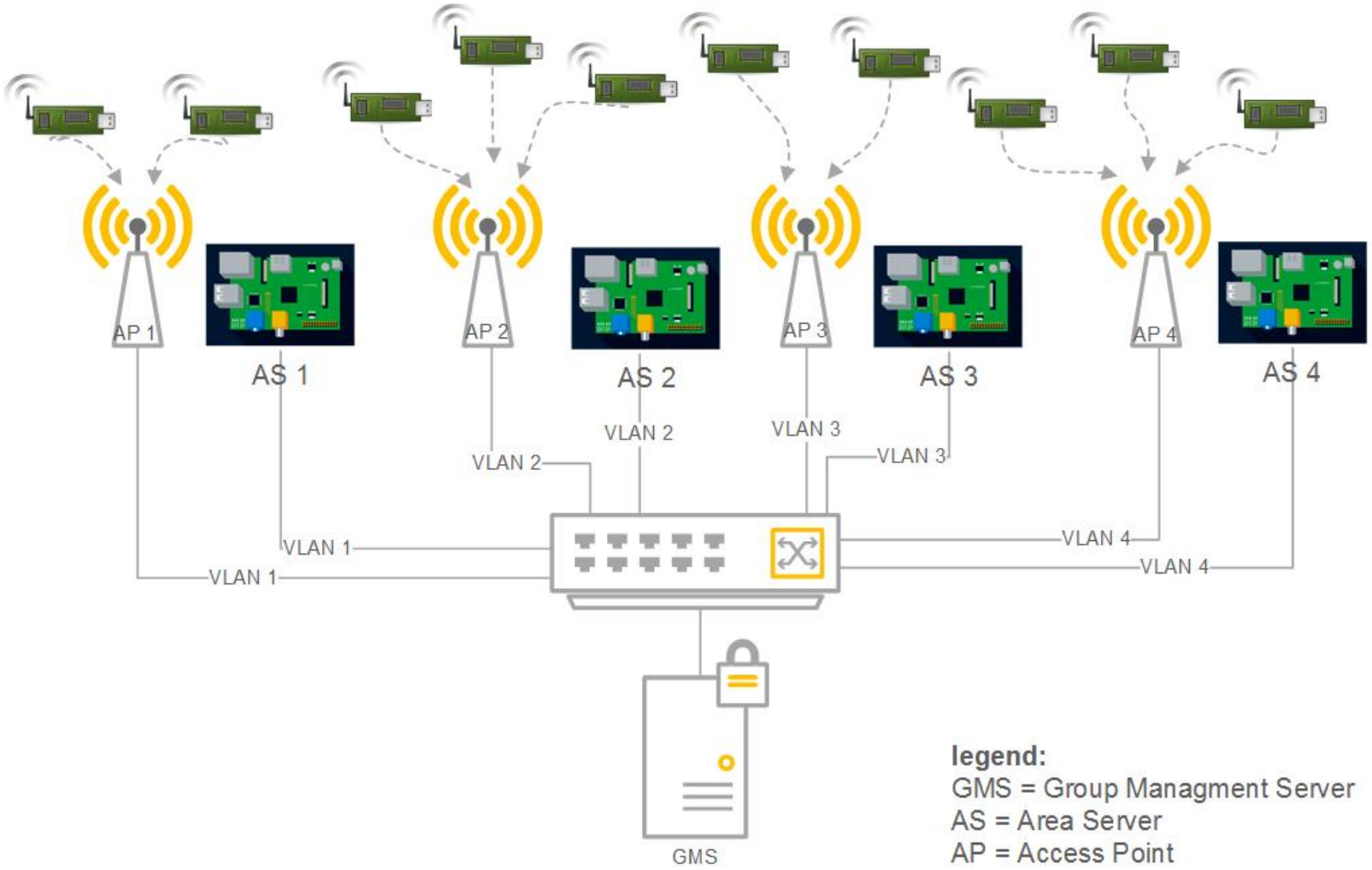
Tobias Guggemos

MNM-Team

Ludwig-Maximilians-Universität München

http://www.mnm-team.org/~guggemos

Testbed


AP 1
AP 2
AP 3
AP 4
AS 1
AS 2
AS 3
AS 4
VLAN 1
VLAN 2
VLAN 3
VLAN 4
GMS
legend:
GMS = Group Managment Server
AS = Area Server
AP = Access Point