FFI Forsvarets forskningsinstitutt

Identity Management and Integrity Protection in Publish-Subscribe systems

Anders Fongen and Federico Mancini
Norwegian Defence Research Establishment

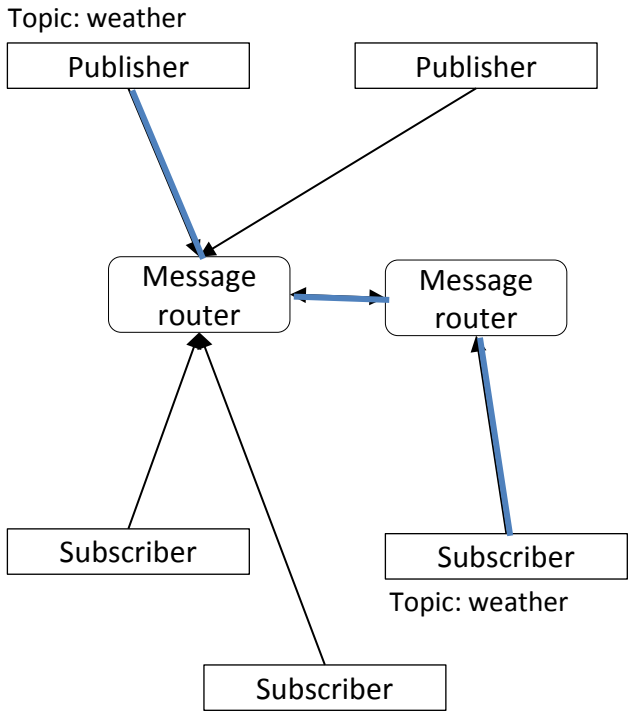
Outline

- Introduction to PubSub
- PubSub security problems
- Outline of the PubSub implementation
- Operational details
- Trusted Binding of Message Router operation
- Conclusions and future work

Principles of PubSub

- Messages are not individually addressed
- Routed from producer to receivers based on content
  - aka content routing
  - content metadata (topics)
- Publications are annotated with *topics*
- Receivers *subscribe* to topics

- Message transport is *asynchronous*
- Scales better
  - employs multicast topologies
- Smaller resource consumption
  - Messages are queued outside the hosts



PubSub security

Problems:

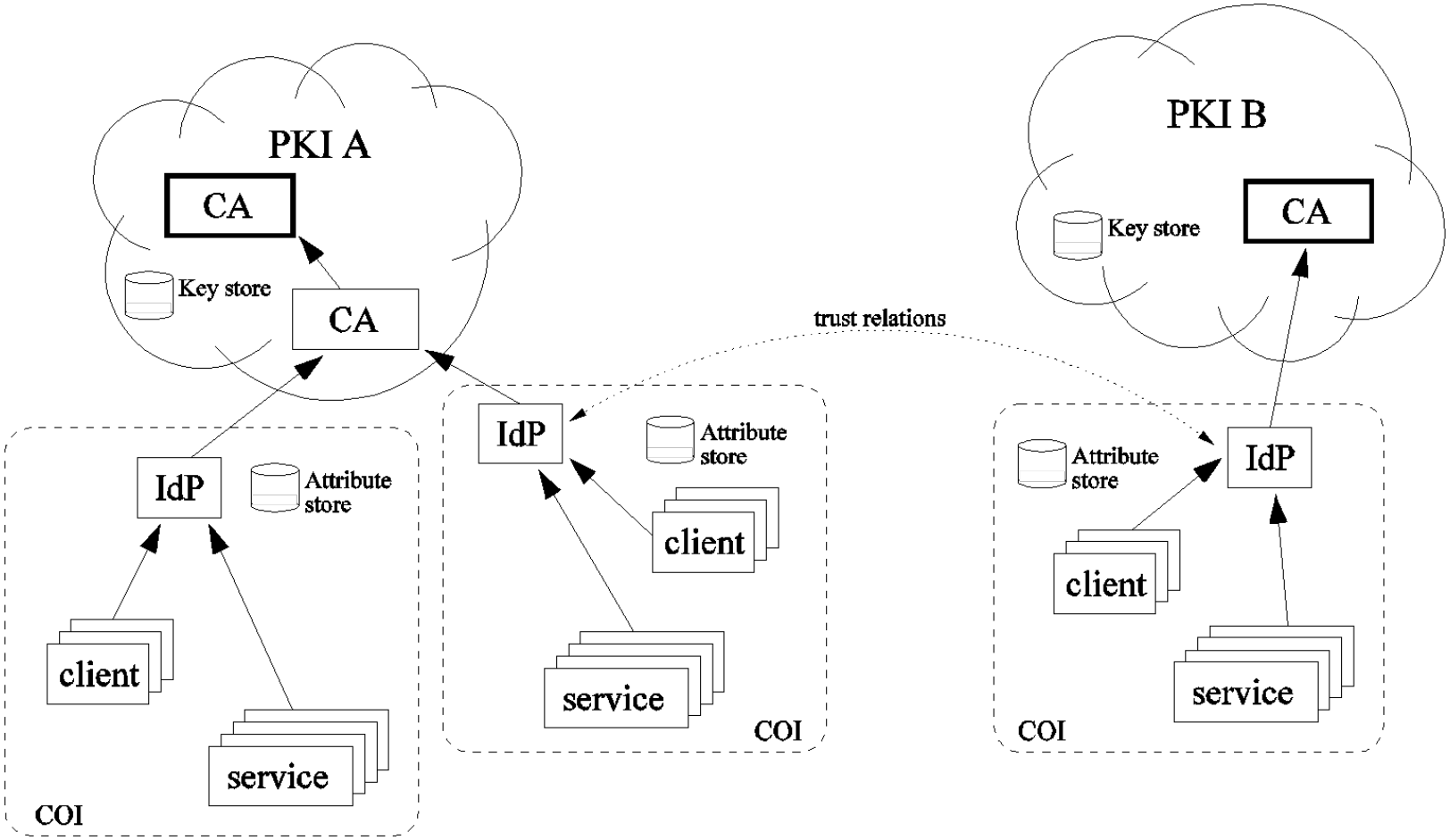
- Is the published information authentic and unmodified?
- Who is the publisher, is it authorized?
- Will the published information only reach authorized subscribers?
- Who operates the message routers? Are they operating correctly?

Principles:

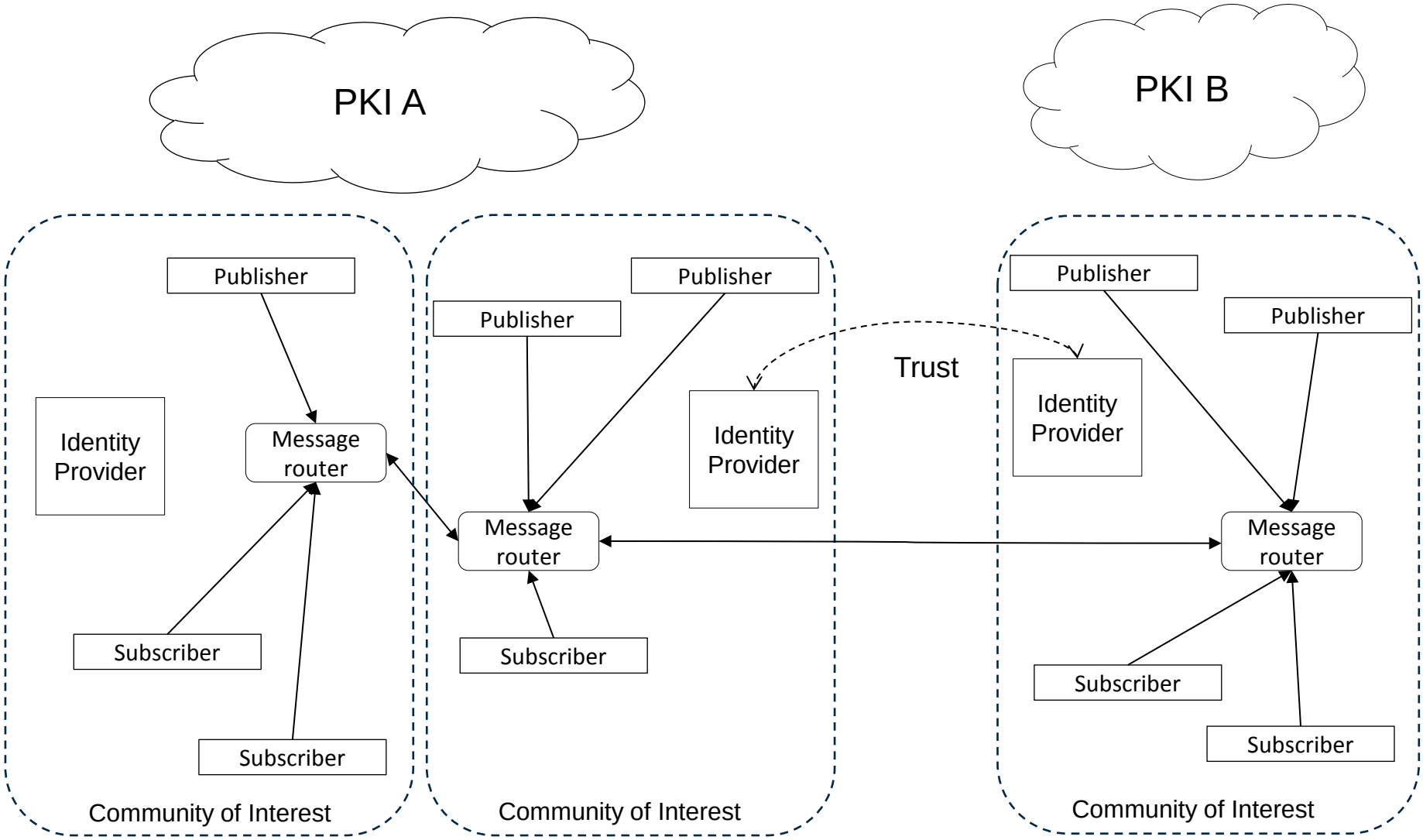
- The confidentiality is the concern of the *Publisher*
  - should be able to express *subscriber requirements*
- The integrity is the concern of the *Subscriber*
  - should be able to express *publisher requirements*
- The correct distribution of messages based on pub-sub requirements is responsibility of the *Message Routers*

Need to identify and authenticate who is generating, transporting and consuming the information: USE OF IDENTITY MANAGEMENT

Components and structure of an IdM



Extending the PubSub network with Identity Management

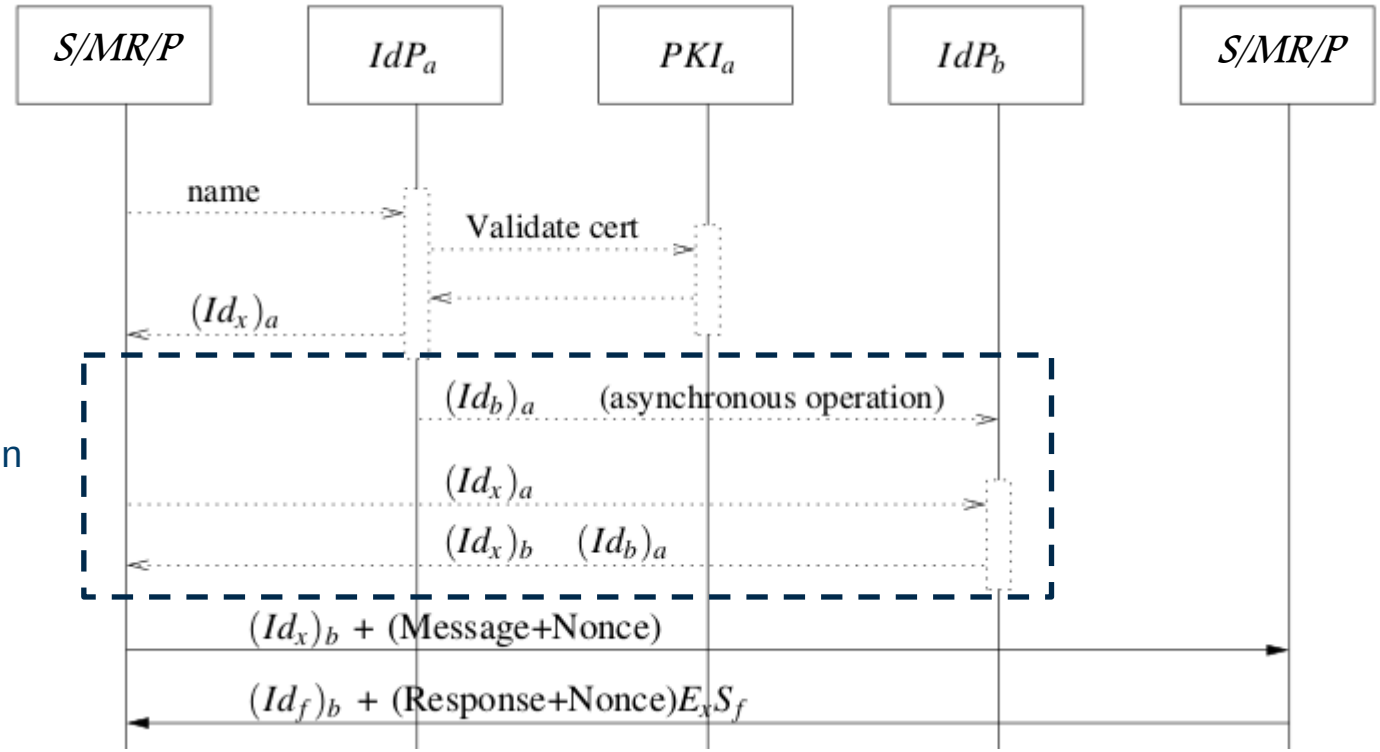


Relations between IdM and PubSub security

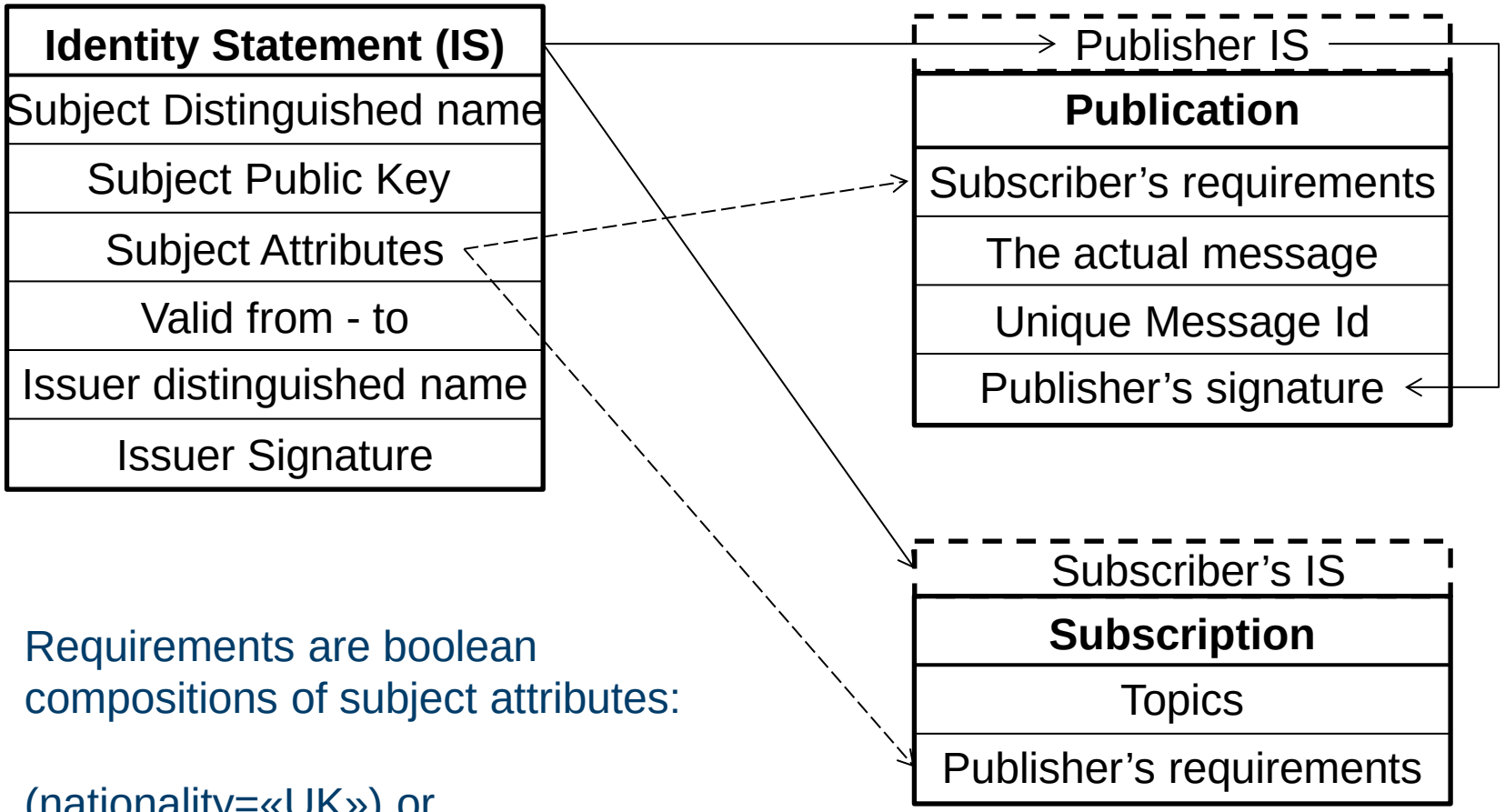
- An IdM issues *Identity Statements* which
  - bind keys and attributes to an identity
  - identity is associated with a subject
- Keys are used to provide subject authentication
  - through a proof-of-possession principle
- Attributes can be interpreted as roles/properties of the subject
  - can be used to represent *authorization*
  - and support the *access control* decisions
- With a trust relation between IdM authorities
  - access control decisions can be made on “foreigners”
  - provided that the attribute “vocabulary” is harmonized
- The correctness of keys and credentials is the responsibility of the *Authority*
  - establishes identities, issues and revokes keys and credentials

Secure PubSub protocol: Authentication

For cross-domain operations



Identity statements, subscriptions and publications



Requirements are boolean compositions of subject attributes:

(nationality=«UK») or
(sec_clearance=«NATO Secret»)

Secure PubSub protocol: Routing tables

- Message routers (MR) exchange *aggregated subscriptions*
  - the “sum” of its clients' subscription (topics+requirements)
- Aggregated subscriptions are flooded in the MR network in order to build *forwarding tables* in each MR
- The functions *merge* and *spill* are defined as follows:

$$c = merge(a, b) \qquad P \supseteq C \supseteq A \cup B$$

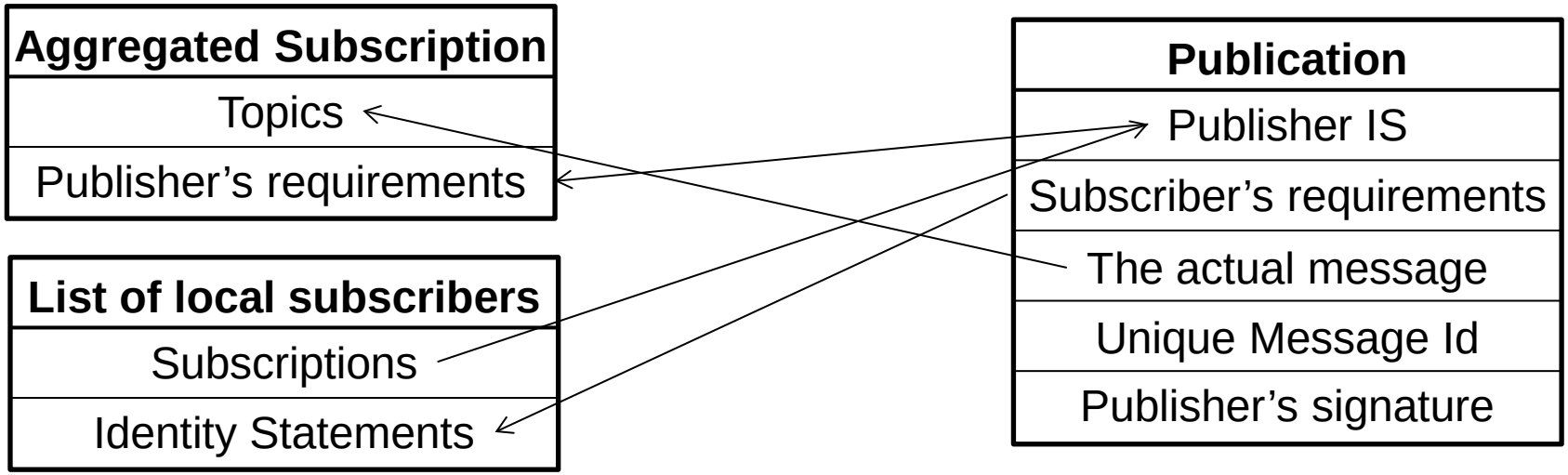
$$spill(a, b, c) = \{x \mid x \in C, x \notin (A \cup B)\}$$

Aggregated Subscription
Topics
Publisher’s requirements

Secure PubSub protocol: Message routing

The MR matches received publications to its aggregated subscription. This is formally defined by a *match* function:

$$A = \{p \mid match(a, p) = true\}, p \in P$$



If A is not empty, then it is forwarded to neighbouring MRs and possibly to the subscribers directly connected to this MR, if their attributes match the publisher requirements.

Message routers integrity

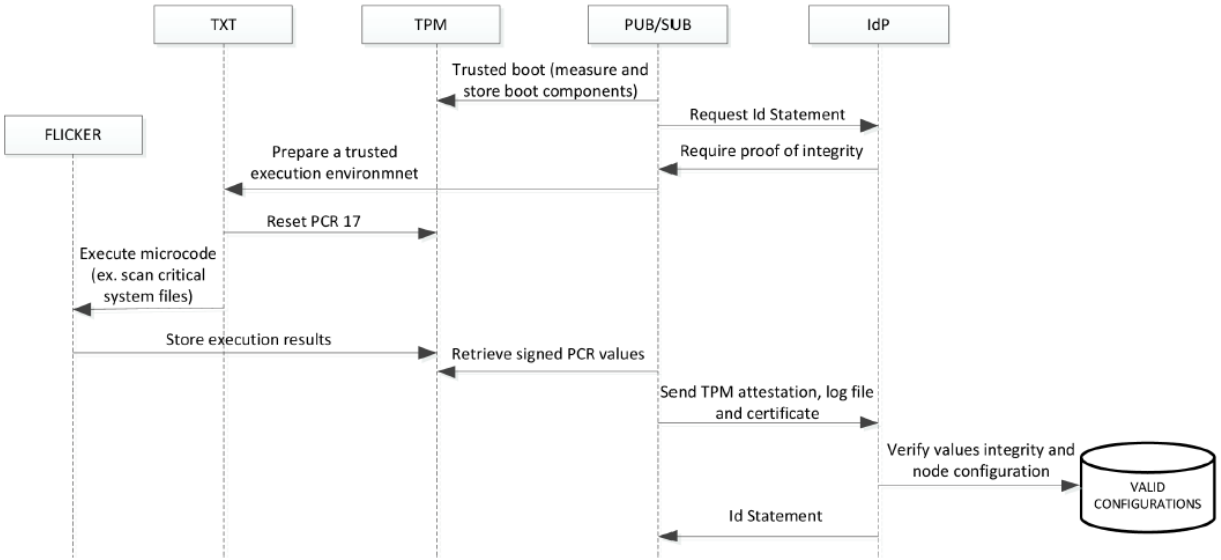
- The message router's integrity is critical for this security model to work.
- The responsibility for message confidentiality and integrity lies with the message routers.
- Therefore we need to trust the message routers to perform the attribute verification correctly and not to tamper with publisher certificates.

Possible threats:

- If the MR code is compromised it can deliver messages to subscribers without the correct attributes, or from a non-reliable publisher
- Unauthorized subscribers or publishers can connect to compromised message routers and read/send messages
- If a publisher IS can be forged by a MR, the message integrity can be compromised

Increase integrity with TPM

- Forging an IS is extremely difficult, and without it any modification to a message can be detected also by a subscriber.
- In order to guarantee the correct operation of a MR, we can use a TPM to seal a predefined configuration, where the code performing the message verification and distribution has been verified.



Conclusions

- The IdM can offer authentication and access control through the Identity Statements issued to all entities involved in the message exchange.
- Identity Statements can be easily extended with attributes that can be used to express subcribers and publishers requirements.
- Message routers can guarantee confidentiality by not delivering messages to subscribers that do not match the publishers requirements. At the same time message integrity can be guaranteed by delivering to subscribers only messages published by publishers they trust.
- Aggregated subscriptions based also on attributes can contribute to stop unauhtorized messaged early in the process. Hence avoiding to waste bandwidth and reducing the exposition of messages to potentially compromised MRs.
- Cross-domain communication can be performed in a transparent way
- TPM based solutions can increase the MRs integrity

Future work and open problems

- Explore possible efficient implementations of the *merge* function
- Test extensively the actual effect of aggregate subscriptions and attribute verification on message traffic
- Investigate further the use of Trusted computing based solutions for MR integrity