A Case Study in Decentralized, Dynamic, Policy-Based Authorization and Trust Management

Monika Maidl [1], David von Oheimb [1],
Richard Robinson [2], Peter Hartmann [3]

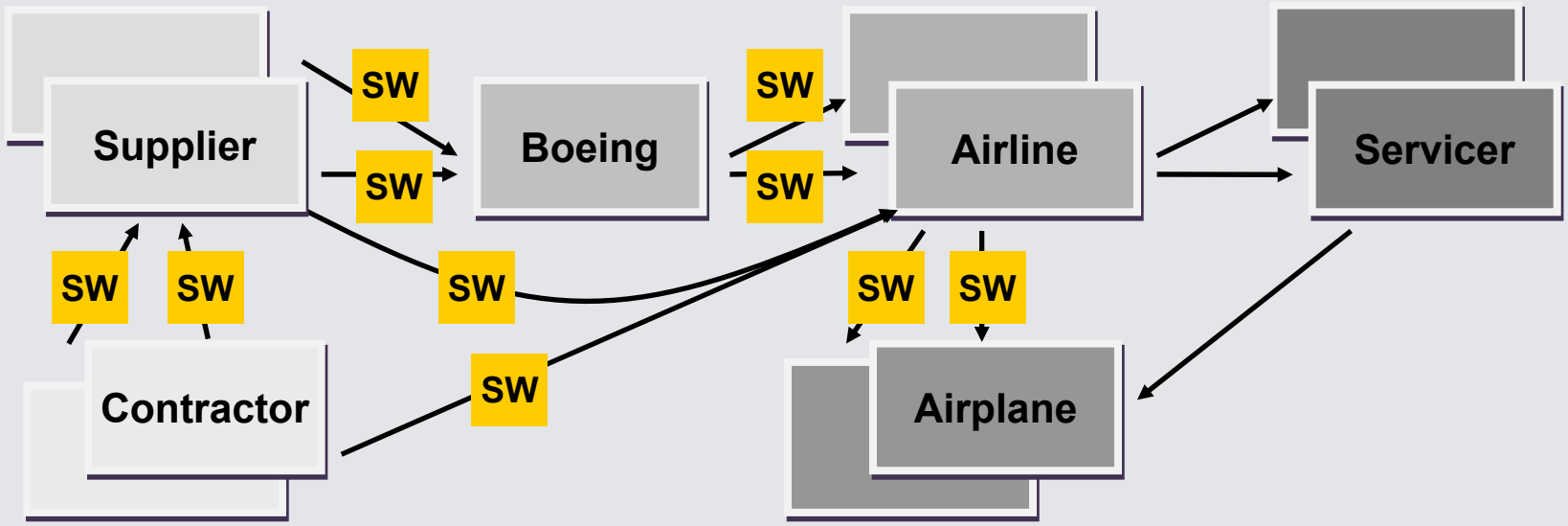
[1] Siemens Corporate Technology, Munich
[2] Boeing Research & Technology, Seattle
[2] Landshut University of Appl. Sciences

STM 2010 Athens, 23 Sep 2010

Overview

- Case Study: Automated software distribution for airplanes
- Dynamic, ad-hoc trust relationships
- Using SecPAL to specify authorization and trust policies
- Conclusion

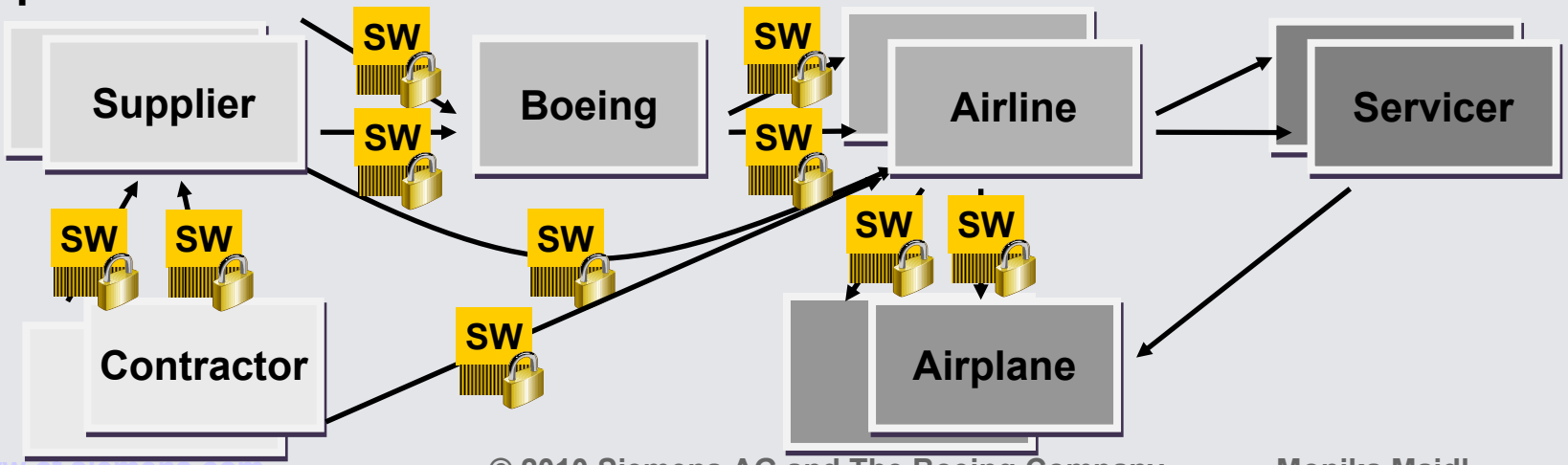
Case Study: Software distribution chain



- Electronic (i.e. network-based) distribution of software for airplanes.
- Software is produced by suppliers of the manufacturer (Boeing) or their contractors
- Airlines receives software parts from Boeing, suppliers or contractors, and send them into airplanes.
- Airlines commissions local service providers to perform the installation.

Case Study: Security aspects

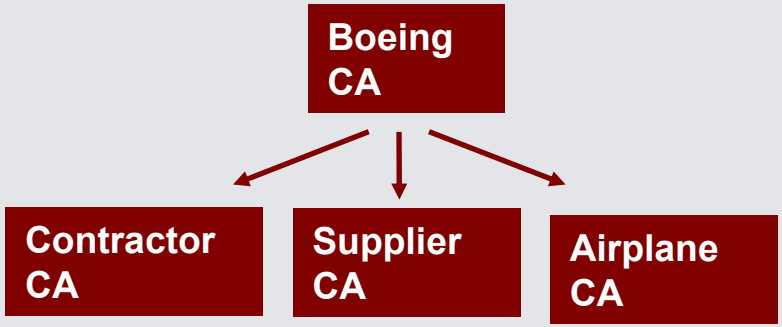
- SW parts in the airplane might perform safety-critical tasks, hence the SW distribution has to be secure.
- Security requirement: Only unmodified SW parts that have been released by trusted producers are installed in airplanes.
- Hence every party along the distribution chain should **authenticate the senders and check if they are authorized** e.g. to release parts.
- Authentication and integrity can be ensured by **signatures** on SW. **PKI certificates** have to be verified – PKI certificate chains have to be in place.



PKI based stable trust relationships

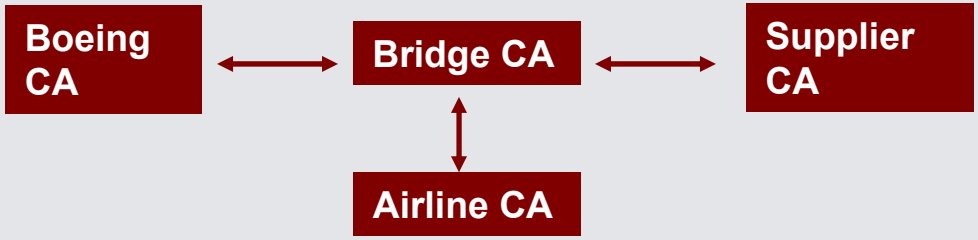
There are several options for building PKI certificate chains.

1. Hierarchical CAs



2. Bilateral cross-certification

3. Bridge CA



Decentralized, dynamic characteristics do not fit with PKI

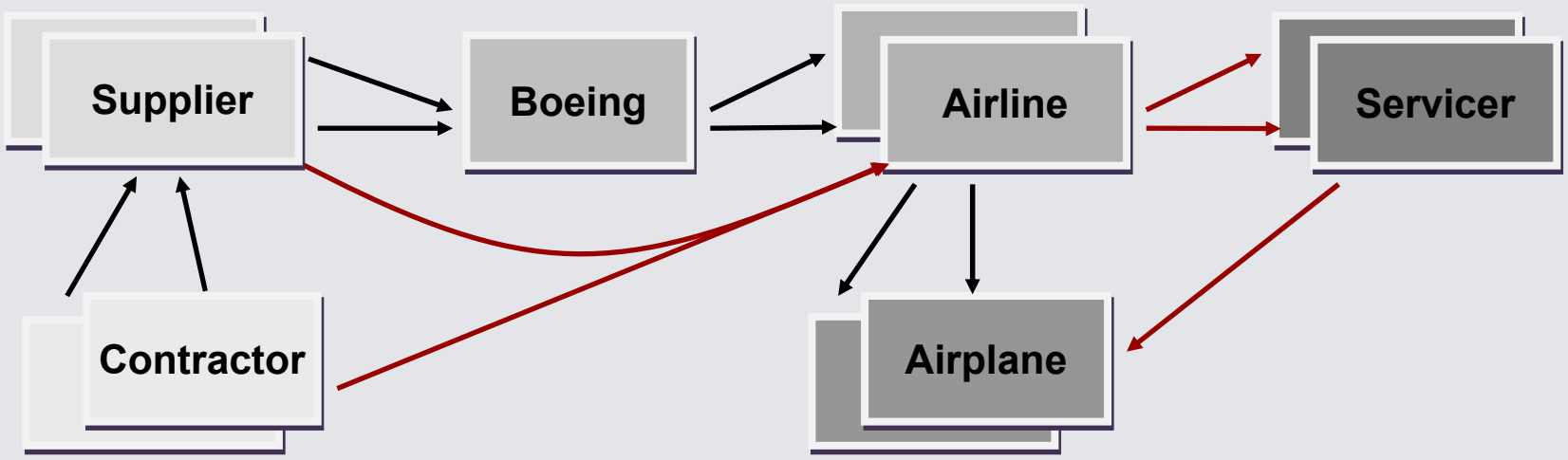
- PKI establishes stable, long-term trust relationships and requires central management:
  - Certificates have a lifetime of one to several years.
  - All options require high organizational effort and costs: Certificate policies have to be agreed and enforced. Certificate Revocation Lists (CRLs) have to be managed.
- The case study is decentralized. The involved parties are globally distributed, highly diverse and their relationships (contractors, service providers) are dynamic. Hence building PKI between all parties is not feasible.
- Ad-hoc: holding partner certificates in local certificate stores. Implicit and very hard to manage!

Overview

- Case Study: Automated software distribution for airplanes
- Dynamic, ad-hoc trust relationships
- Using SecPAL to specify authorization and trust policies
- Conclusion

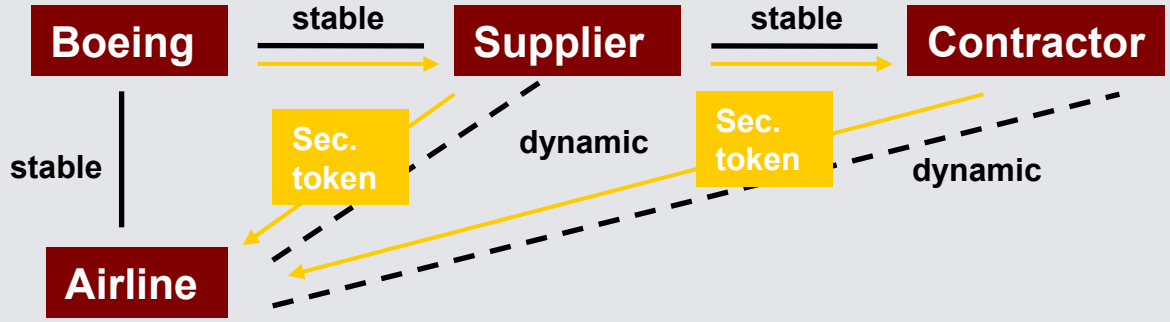
Dynamic, ad-hoc trust relationships in the case study

Stable relationships	Dynamic relationships
Boeing – Airline: Airlines can verify Boeing's certificates. **Airline – Airplane**: The airplane can verify credentials of its airline	**Airline – Suppliers**: Airlines do not manage relationships with suppliers. **Boeing – contractors**: Boeing is not directly involved with contractors. **Airplane – Service providers**: service providers not known by the airplane



Measures to handle dynamic, ad-hoc trust relationships

Stable, long-term trust	Dynamic, decentralized trust
- Authentication by long-term credential (certificate, password) - Incorporated into IT infrastructure (user accounts,..) - Contracts and agreements.	- **Delegated authentication by short-term security tokens**, with a short validity (no revocation required) issued within a stable relationship, and used between decentralized partners. - **Explicit chains of trust**. Dynamic trust relationships are used to establish other dynamic relationships. - **Attribute-based authorization,** using information like roles, context, etc.



Policies to specify authorization and trust

- Conditions and constraints have to be specified explicitly in policies.
  - Which security tokens are accepted?
  - Under which conditions are chains of trusted formed?
  - Which attributes are required to obtain authorization for which actions?
- Policies have to be unambiguous and easy to interpret.
- Automated evaluation of policies.

Overview

- Case Study: Automated software distribution for airplanes
- Dynamic, ad-hoc trust relationships
- Using SecPAL to specify authorization and trust policies
- Conclusion

SecPAL can be used to specify policies for dynamic, decentralized authorization and trust.

BOEING
SIEMENS

- SecPAL is based on logic programming (Datalog):
  - Arbitrary attributes can be defined.
  - Automatic reasoning to deduce valid consequences.
- SecPAL offers constructs to specify delegation.
- Example:

o Airline says p is accepted if p is type2-critical AND p is approved.

o Airline says Boeing can say x is a supplier.

o x can say y is a contractor till t if x is a supplier AND currentTime < t.

o y can say p is approved if y is a contractor. Delegation => chain of trust

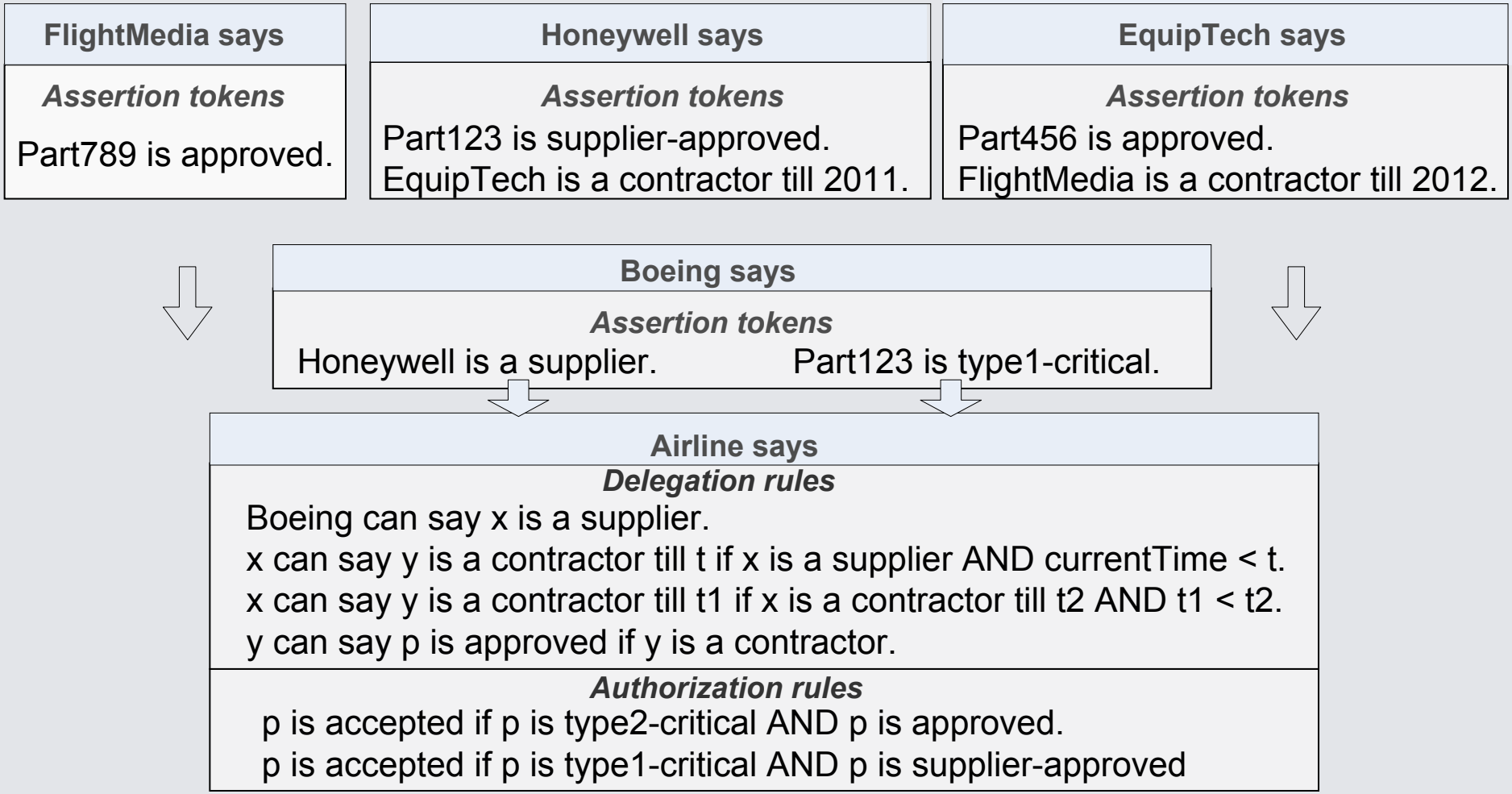
o Boeing says Honeywell is a supplier.

o Honeywell says EquipTech is a contractor.

o EquipTech says Part456 is approved. Security tokens with attributes

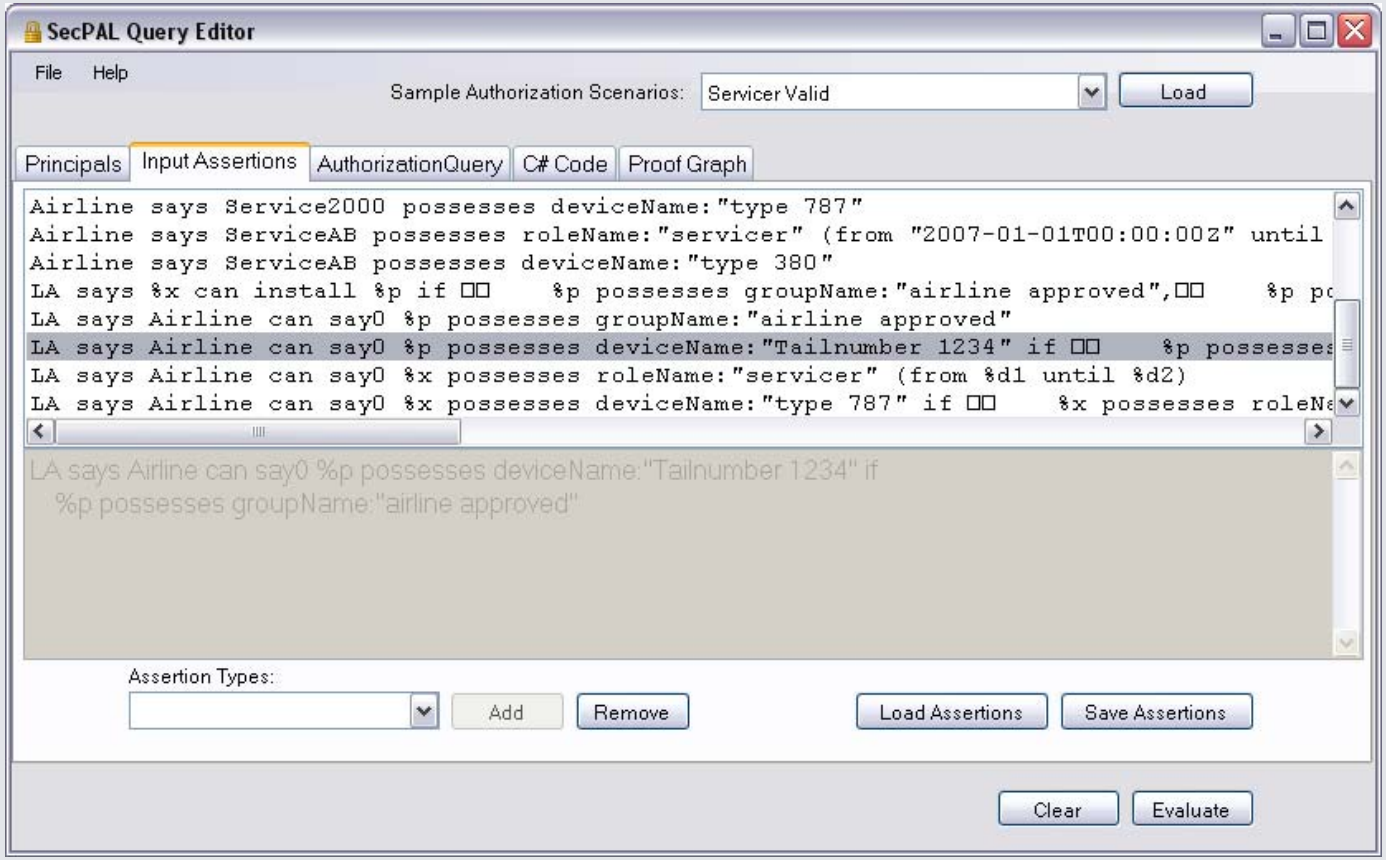
Request: Part456 is accepted?

SecPAL policy for authorization of suppliers and contractors



Demonstrator

Implementation of SecPAL query evaluation is available: C# class libraries and a GUI (SecPAL Query editor) to start evaluation and examine proof trees.



Related work

- The SAML protocol and SOAP message security (WS-*) are established examples of token-based security models.

  (Different goals than SecPAL, namely Single Sign-On, Identity Federation and SOAP message authentication and protection).

- SAML assertions are a widely-used from of security tokens.
  - Attributes can be used in SAML assertions.
  - SAML can be combined with XACML (eXtensible authorization markup language) to specify centralized authorization. No delegation constructs.
- A range of logic-based authorization policy languages have been proposed for differing purposes.

Conclusion

- Our case study demonstrates the demand for a decentralized authorization policy language for **IT system with networked devices in the field performing critical tasks.**
  (Other examples: automobiles and public transport, energy distribution, programmed machine tools, medical devices …)
  - PKI infrastructure including all parties is not feasible.
  - Inserting certificates into local certificate stores is hard to manage
- SecPAL is suitable to express decentralized authorization and trust policies as required by our case study.
- The resulting policies are easy to grasp for non-experts.
- Standardization and binding to existing transport protocols would be required to promote usage.

BOEING

SIEMENS

Thank you for your attention.

Questions?