

Mobile Adventure

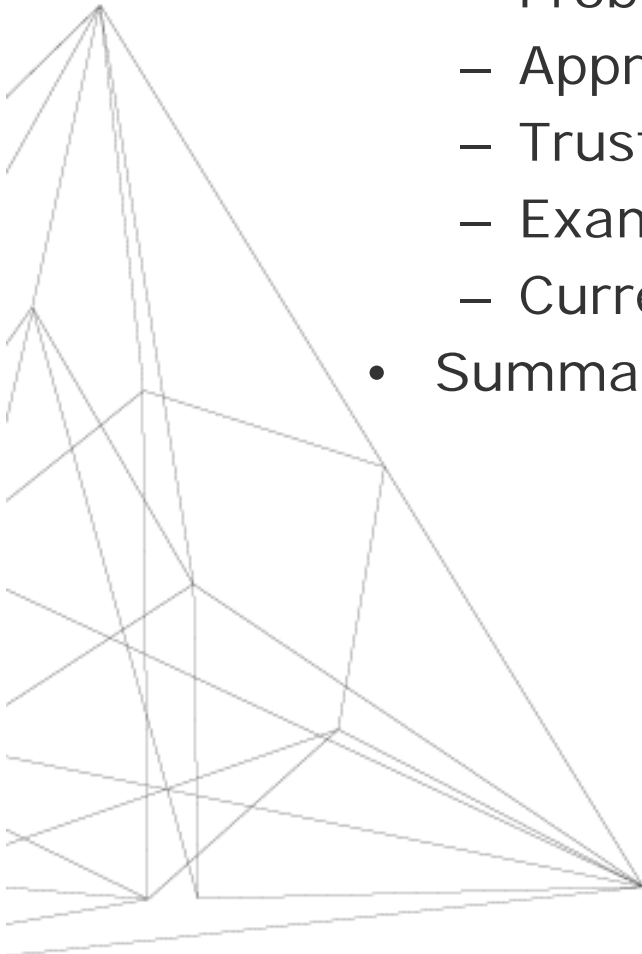



Context-Awareness, Trust and Security

Safe-NL Workshop, Nov 18, 2005

Sven Lachmund

DoCoMo Euro-Labs

- Meaning of trusted context information
 - Context-Aware Trust and Security
 - Problem statement
 - Approach
 - Trust evaluation
 - Example
 - Current state
 - Summary and conclusions
- 
- 

- European research project



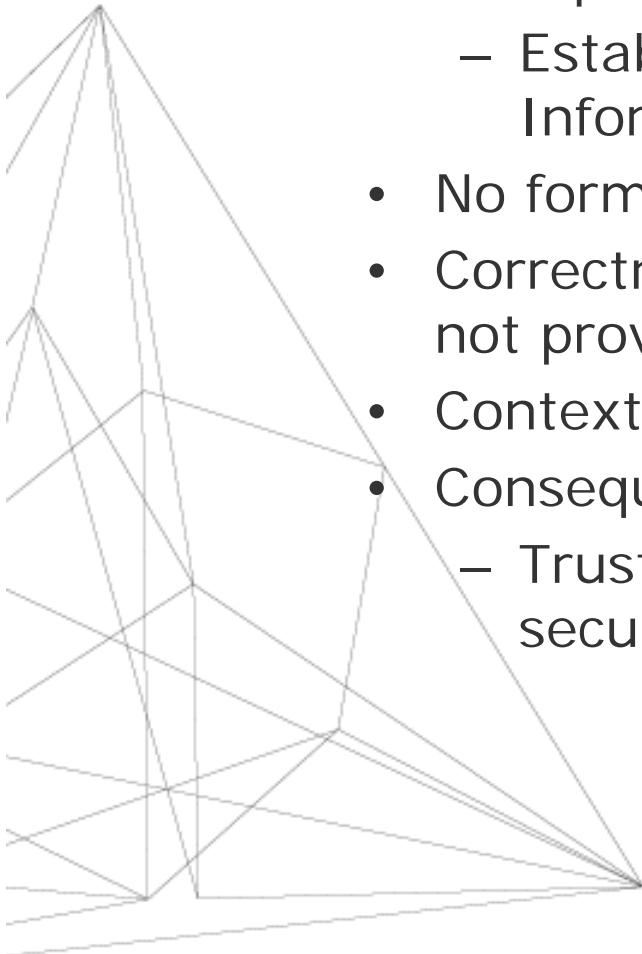
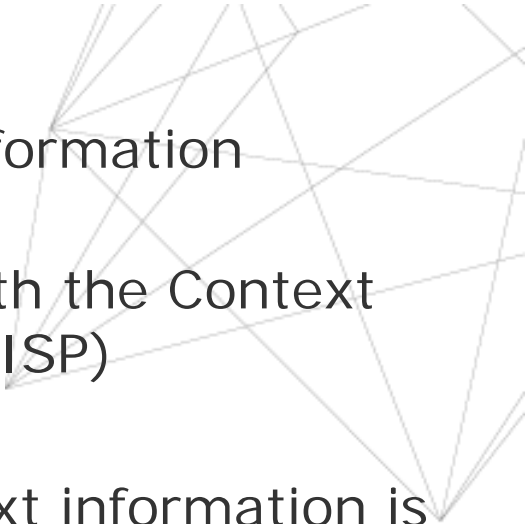
MOSQUITO

Mobile workers' secure business applications in ubiquitous environments

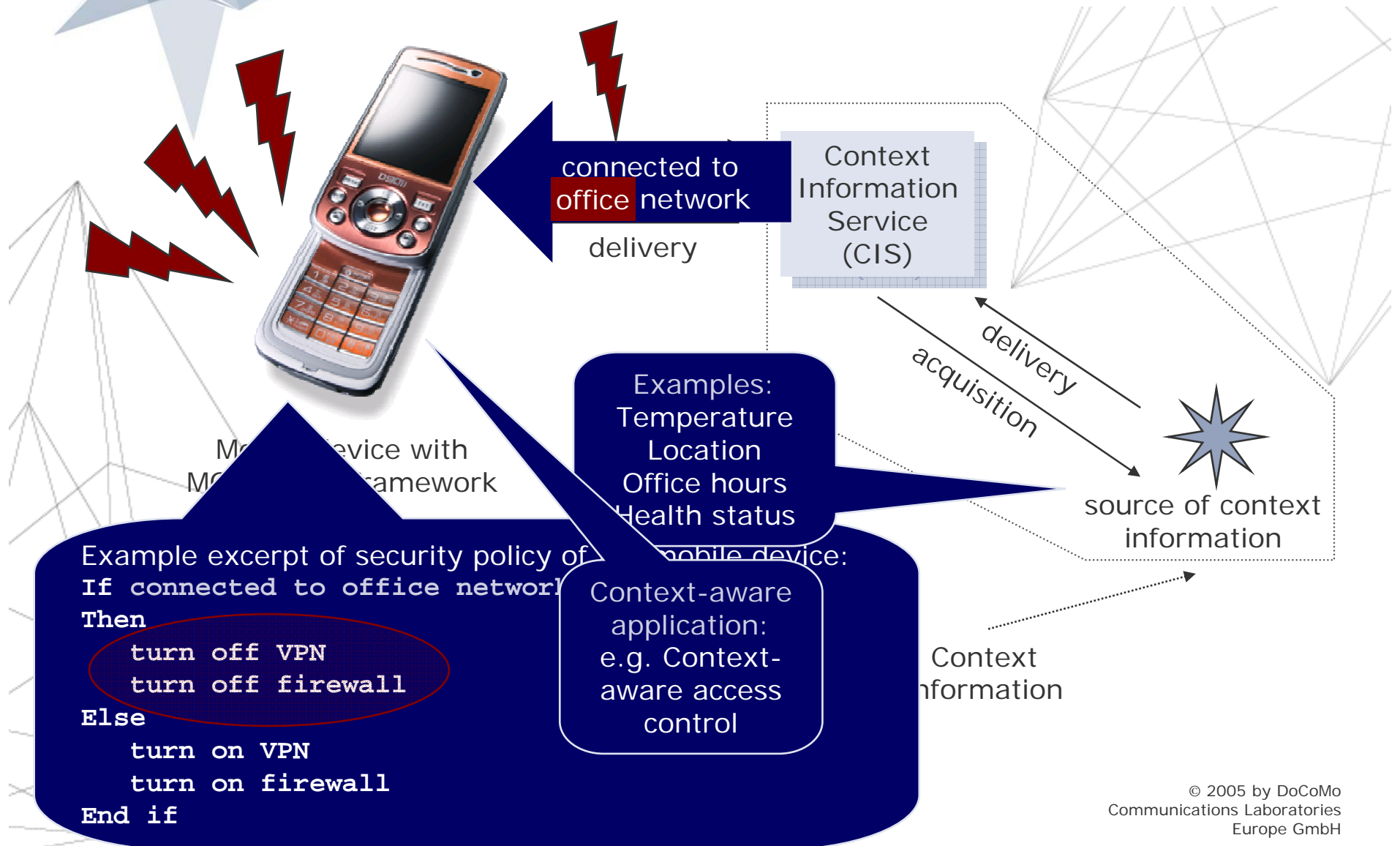
- Consists of eight partners from industry and academia
- Started September 2004
- Ends august 2006

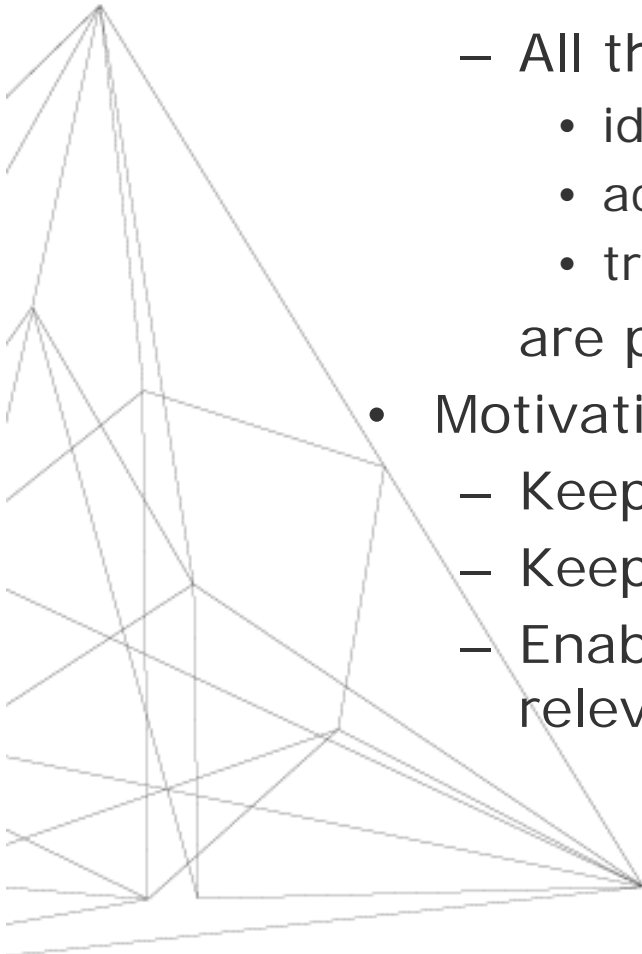
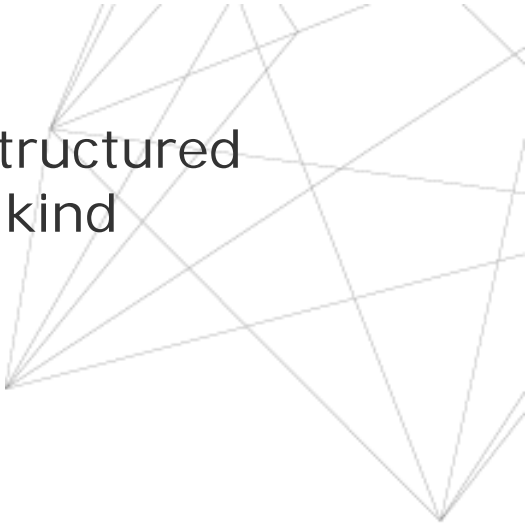
- Providing a security framework for business applications for mobile devices
 - Services oriented
 - Acts on message level
 - Provides
 - Security mechanisms as APIs and Web Services
 - Context information acquisition and delivery
 - Trust evaluation of Context information
 - Context-aware security policy enforcement during execution time
- Work comprises
 - Specification of architecture and services
 - Implementation of a demonstrator

My part

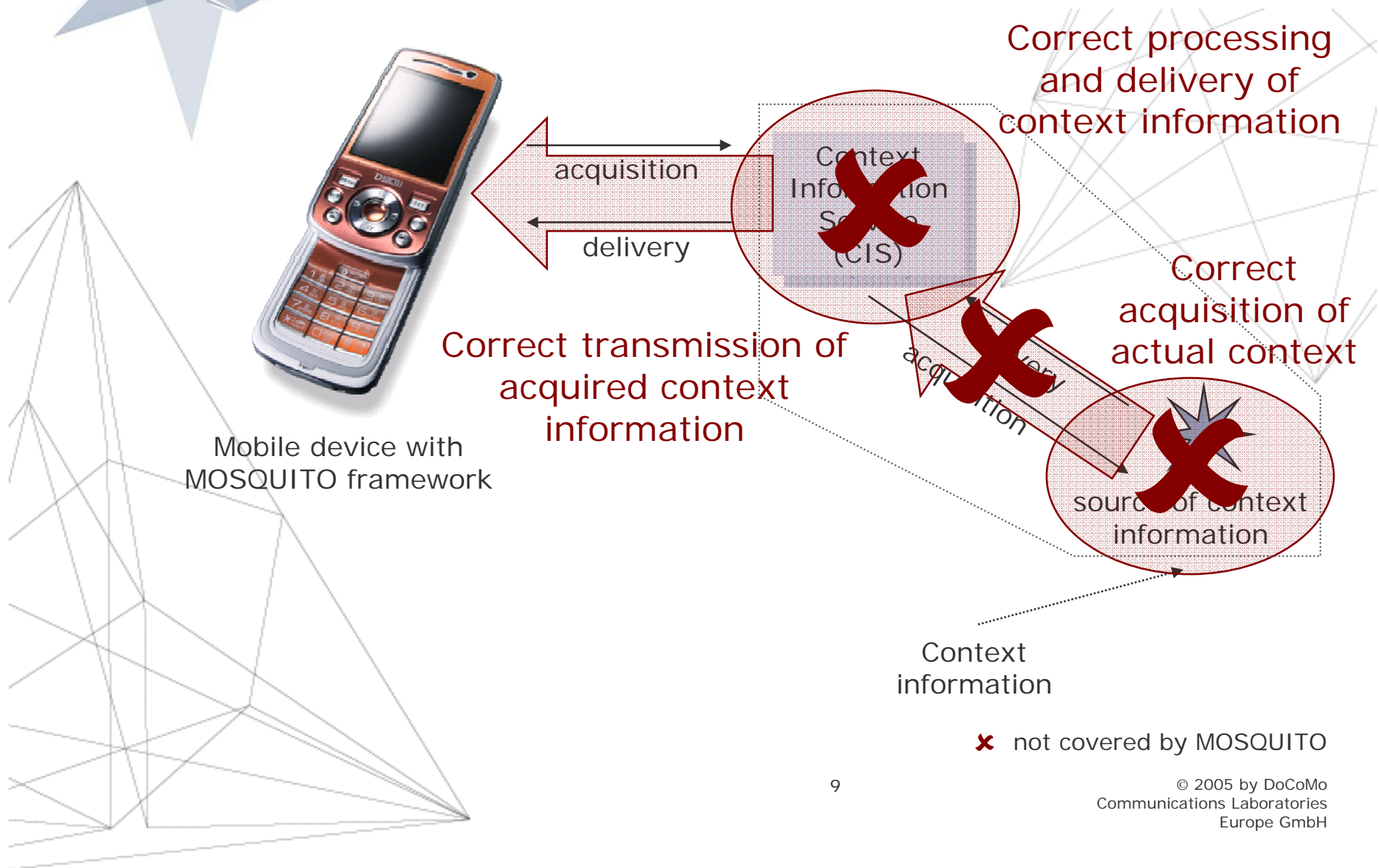
- 
- 
- Trusted context information
 - Gain confidence that context information represents the actual context
 - Establish a trust relationship with the Context Information Service Provider (CISP)
 - No formal model is applied
 - Correctness of acquisition of context information is not proven
 - Context information (CI) is limited to facts
 - Consequences
 - Trusted context information can be used for security relevant decisions

Mobile Adventure Problem Statement

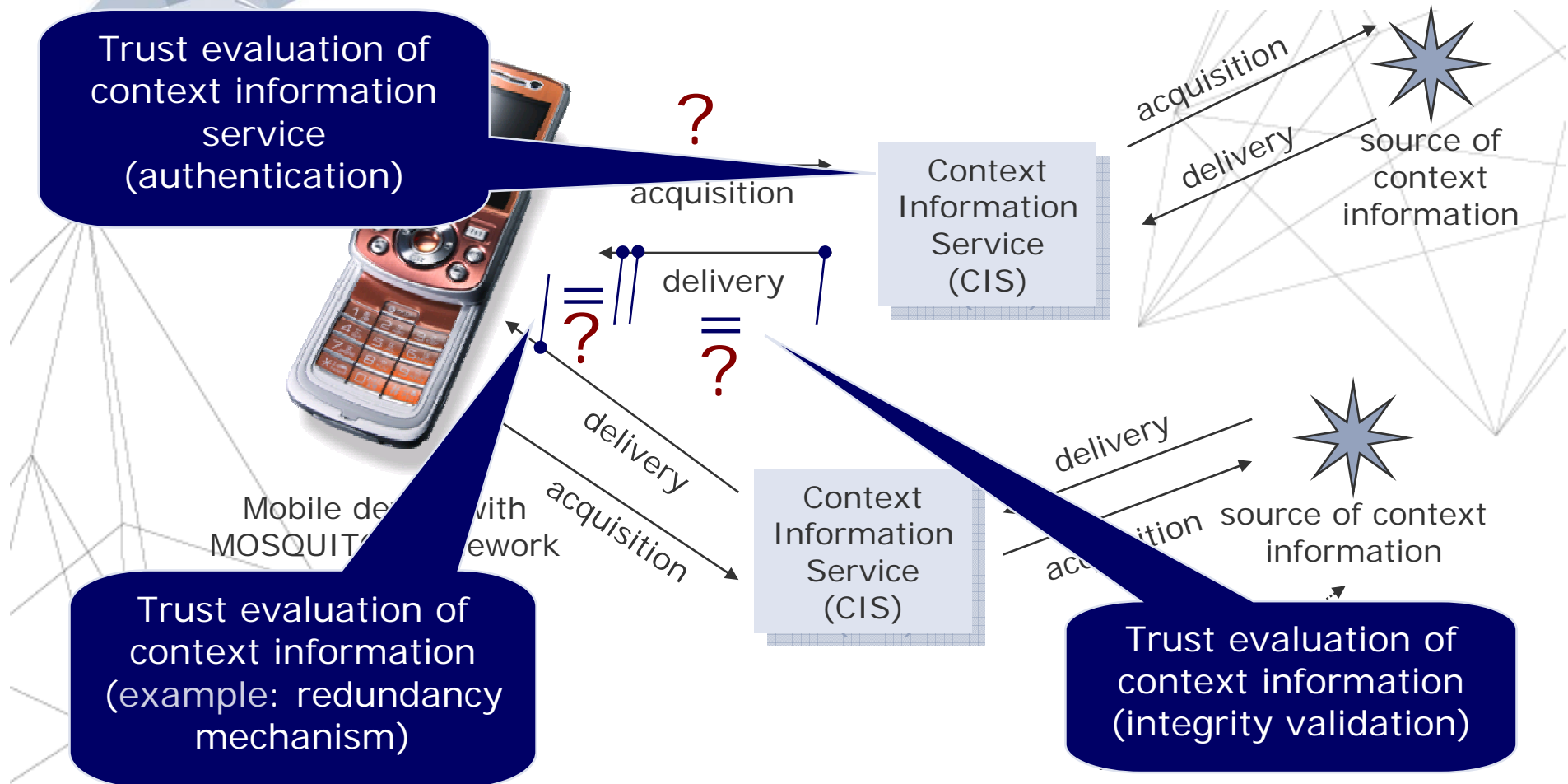


- 
- 
- Objectives
 - Enable applications to acquire structured context information (CI) of any kind
 - All the necessary tasks such as
 - identification of providers
 - acquisition of CI
 - trust evaluation of CIare performed in the framework
 - Motivation
 - Keep trust establishment out of the applications
 - Keep CI acquisition out of the applications
 - Enable applications to use CI for security relevant decision making

- Provide service within MOSQUITO framework that provides context information
 - Introduce **Context-Aware Trust and Security (CATS)**
- Deal with **trust evaluation** within CATS
 - Provide an environment where trust evaluation mechanisms can be hooked in and used
 - Evaluation mechanisms are controlled by trust evaluation policies
 - Trust evaluation policies can be provided by CI requesting applications
 - Provide **trusted** context information



- Mobile Device cannot influence/monitor sources of context information
- MOSQUITO does not deal with
 - Use/manage of sources of CI
 - Acquisition of CI from sources of CI
 - Transmission of CI from sources of CI to CIS
 - Processing of CI within CIS
 - Provision of trust evaluation mechanisms
 - Privacy
- MOSQUITO deals with
 - Acquisition of CI from CIS
 - Transmission of CI from CIS

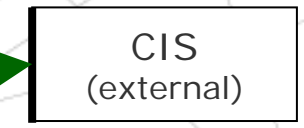
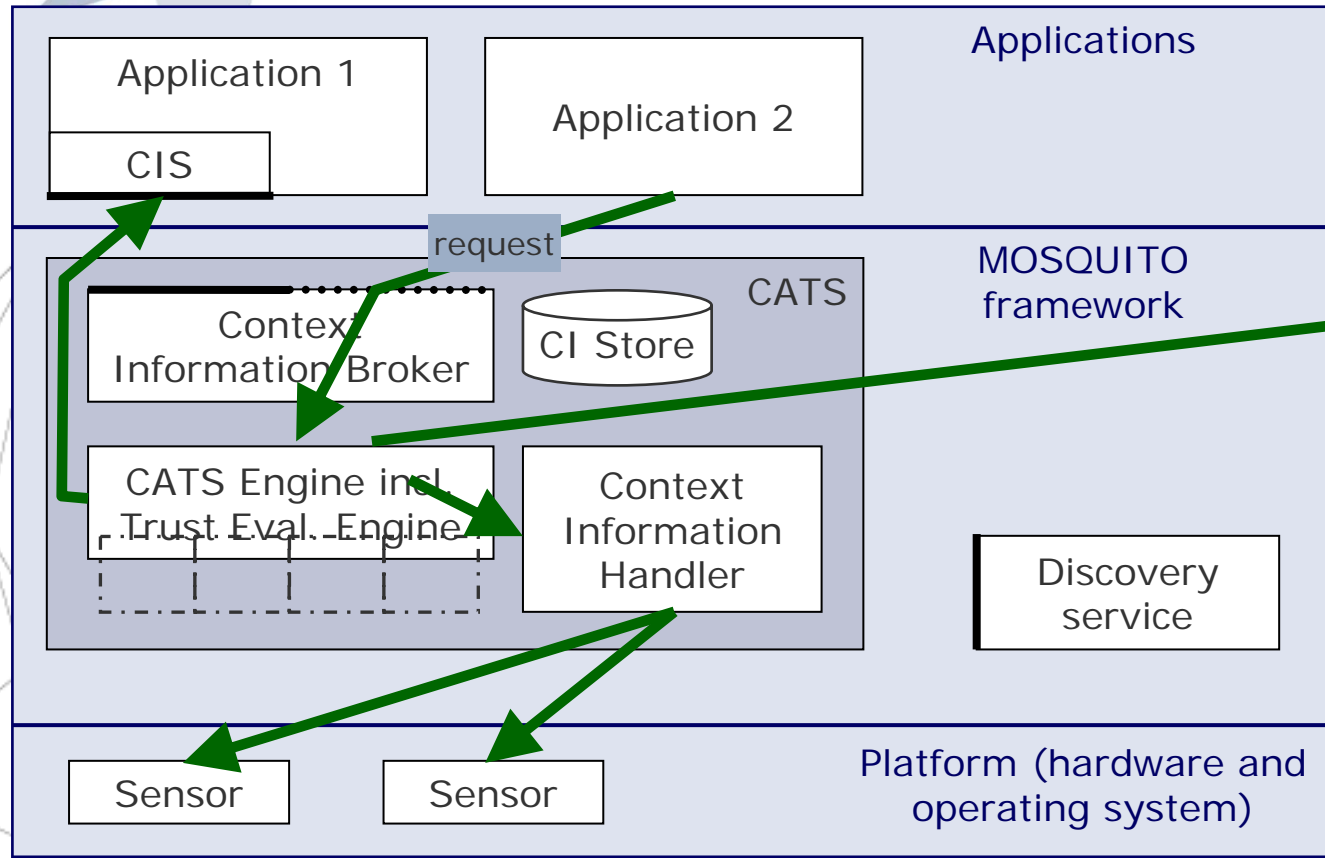


- Trust evaluation makes trusted CI out of CI

- CI could be altered during transmission
- CATS provides **trust evaluation of CISP**
 - Authentication of CIS
 - Gain **evidence** that originating CIS is the expected one
 - Possible trust evaluation mechanisms
 - Digital Signature/Cryptographic mechanisms
 - Reputation/Recommendation
 - Ratio-based/past experience
- CATS provides trust evaluation of CI
 - Integrity validation of CI
 - Gain **evidence** that CI has not been altered during transmission

- Acquisition of CI could be incorrect
- CATS provides **trust evaluation of CI**
 - Analysis of acquired CI
 - Gain **confidence** that acquired CI represents the actual context
 - No proof of correct acquisition
 - Possible trust evaluation mechanisms
 - Redundancy
 - Consistency/History knowledge
- Trust evaluation of CI can also be done by the CIS
 - CIS performs the same analysis as CATS
 - CIS needs to show/prove CATS that it performed these analysis
 - E.g. By Service Level Agreement (SLA)

CATS Architecture Overview

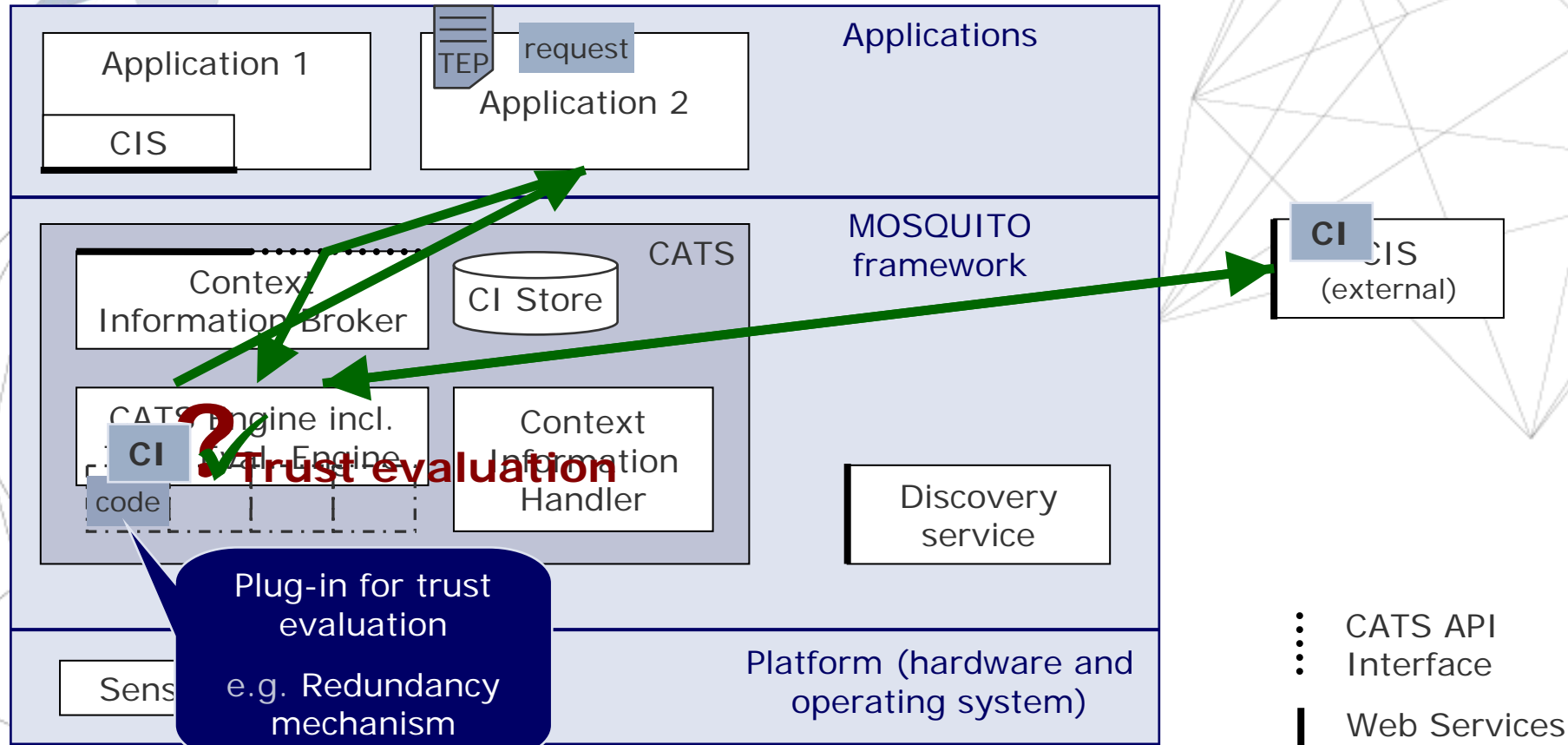


- ⋮ CATS API Interface
- ⋮ Interface
- Web Services Interface
- ⋮ Hook

Device with MOSQUITO framework or Context Information Service with MOSQUITO framework

CIS = Context information service

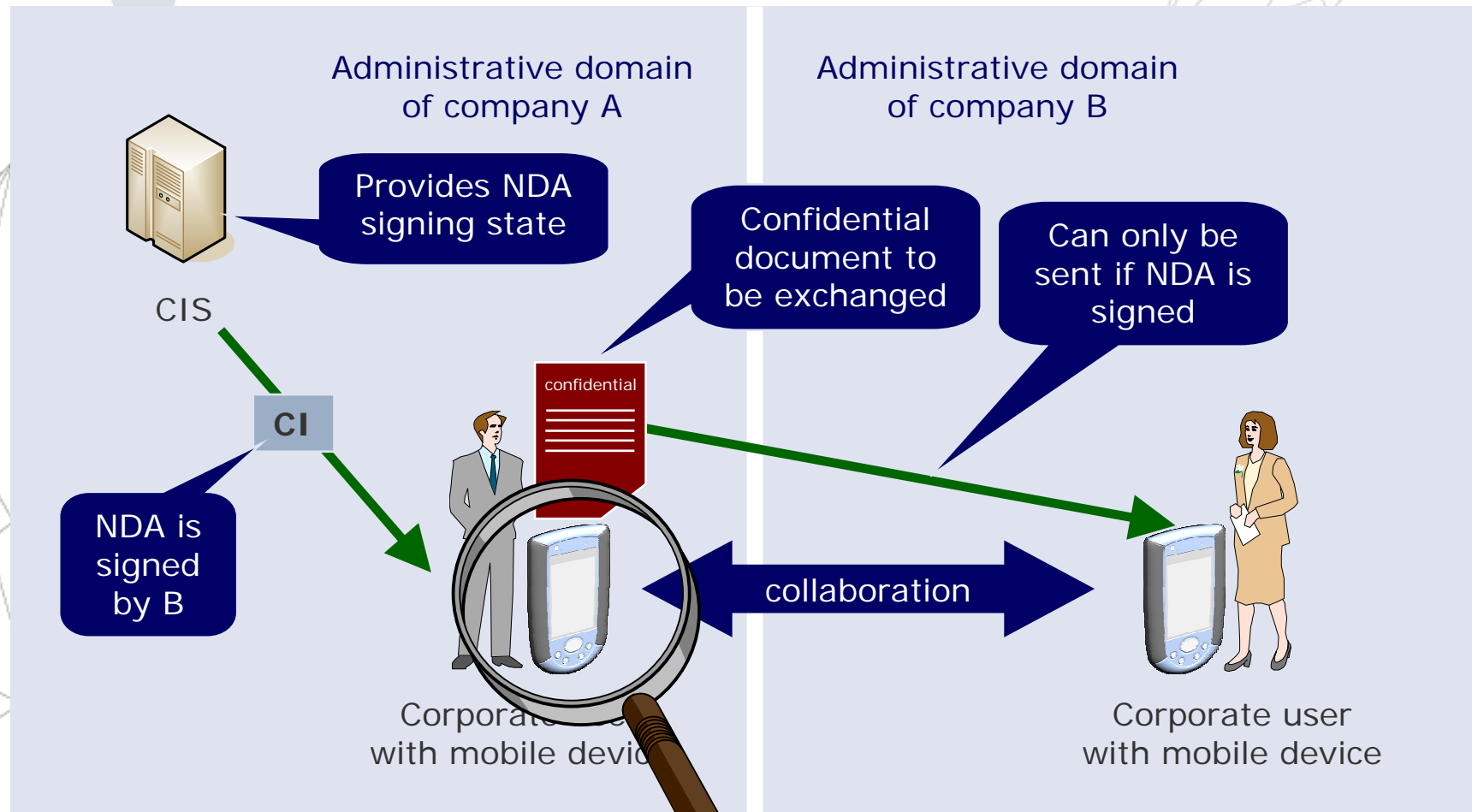
CATS – Concept of Trust Evaluation



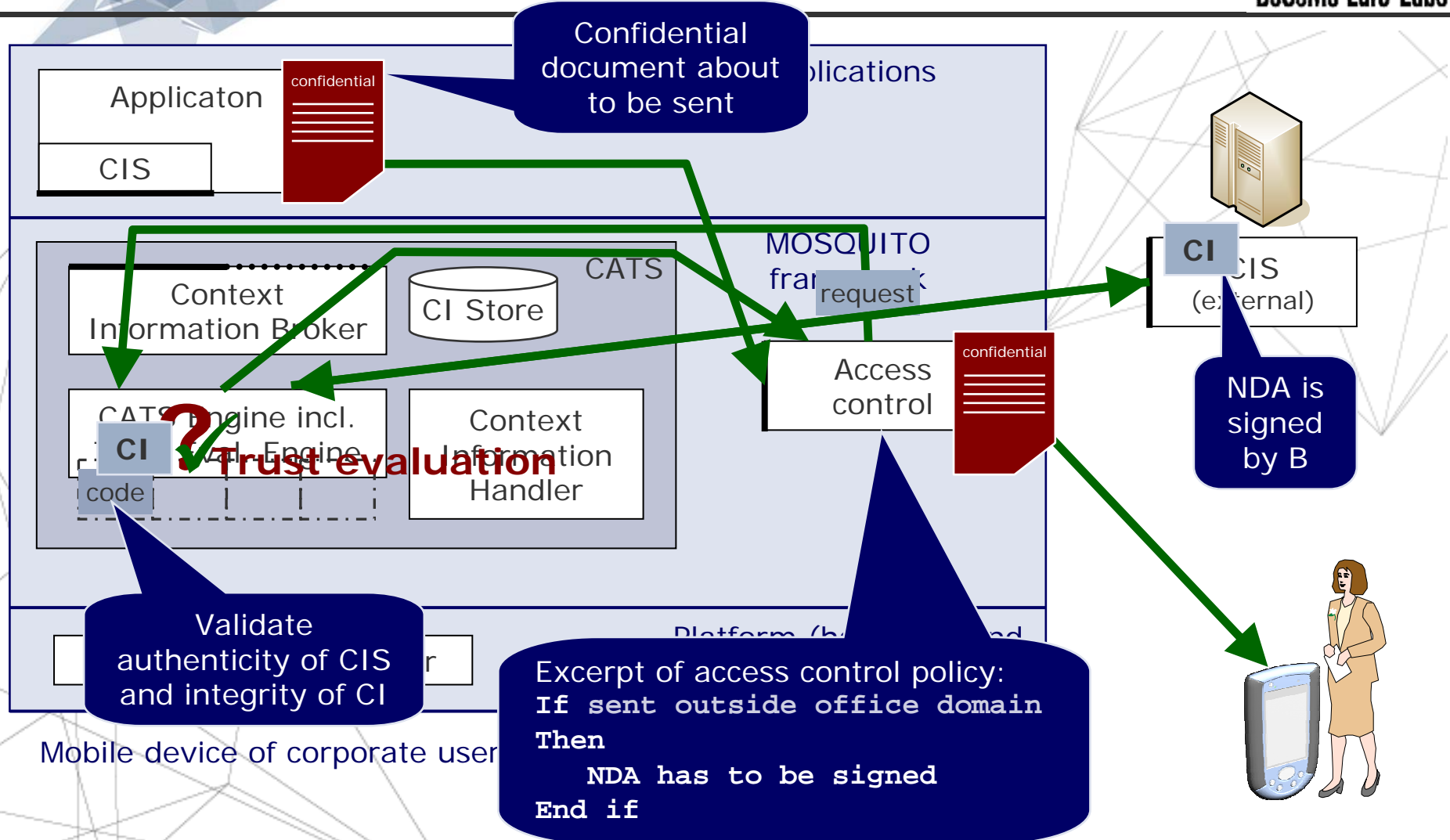
Device with MOSQUITO framework or Context Information Service with MOSQUITO framework

CIS = Context information service
TEP = Trust evaluation policy

- CATS
 - Performs acquisition and delivery of CI and discovery of sources
- Trust Evaluation Engine (component of CATS but functionally independent)
 - Performs trust evaluation of CIS
 - Performs trust evaluation of CI
 - Is controlled by Trust Evaluation Policy (TEP), added to the application
- Application
 - Requests and consumes CI



Example: Send Document Under NDA



CIS = Context information service

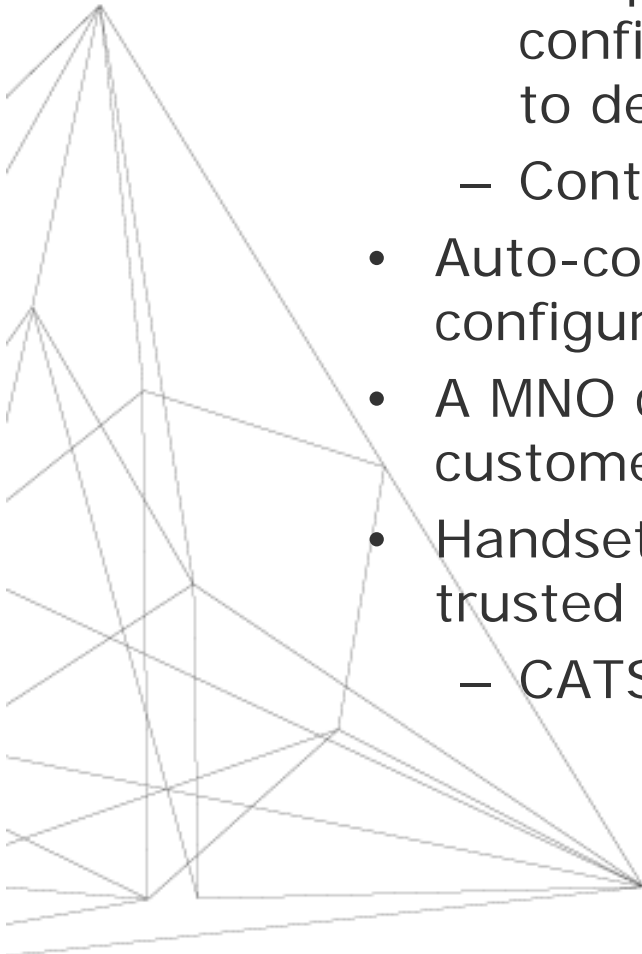
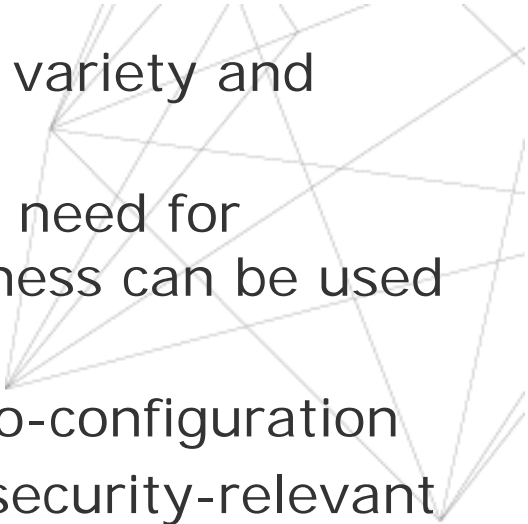
- Provide **trusted** CI to context-aware applications
 - Different scope compared to existing approaches
 - E.g. Context Toolkit, no security considerations
 - E.g. CoBra, access control to CI
 - E.g. Geopriv, privacy and authorisation
 - E.g. Ambient Networks, privacy and authorisation
 - E.g. JCAF, quality of CI
 - Not limited to location

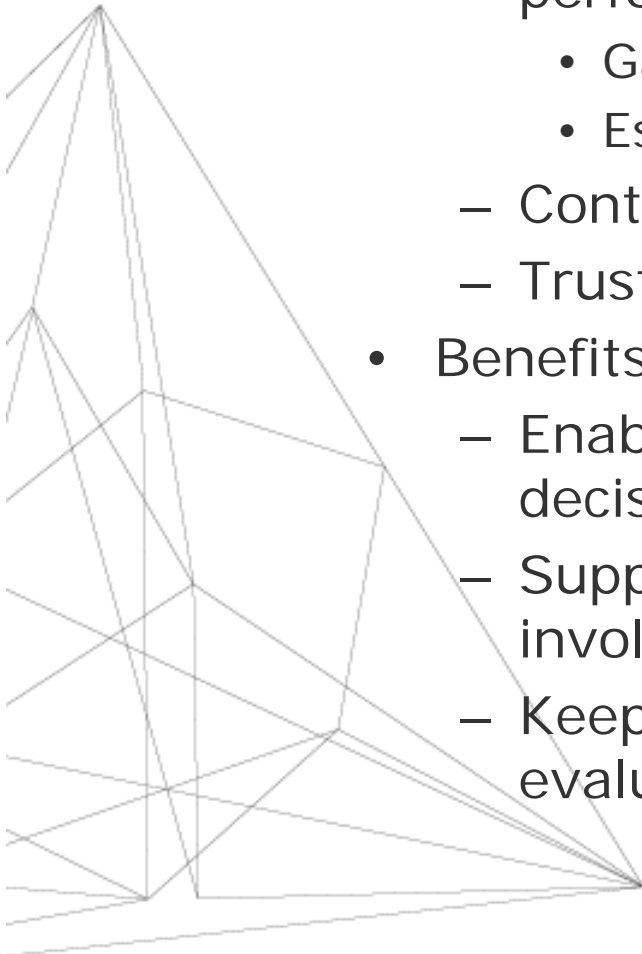
Work package started in December 2004

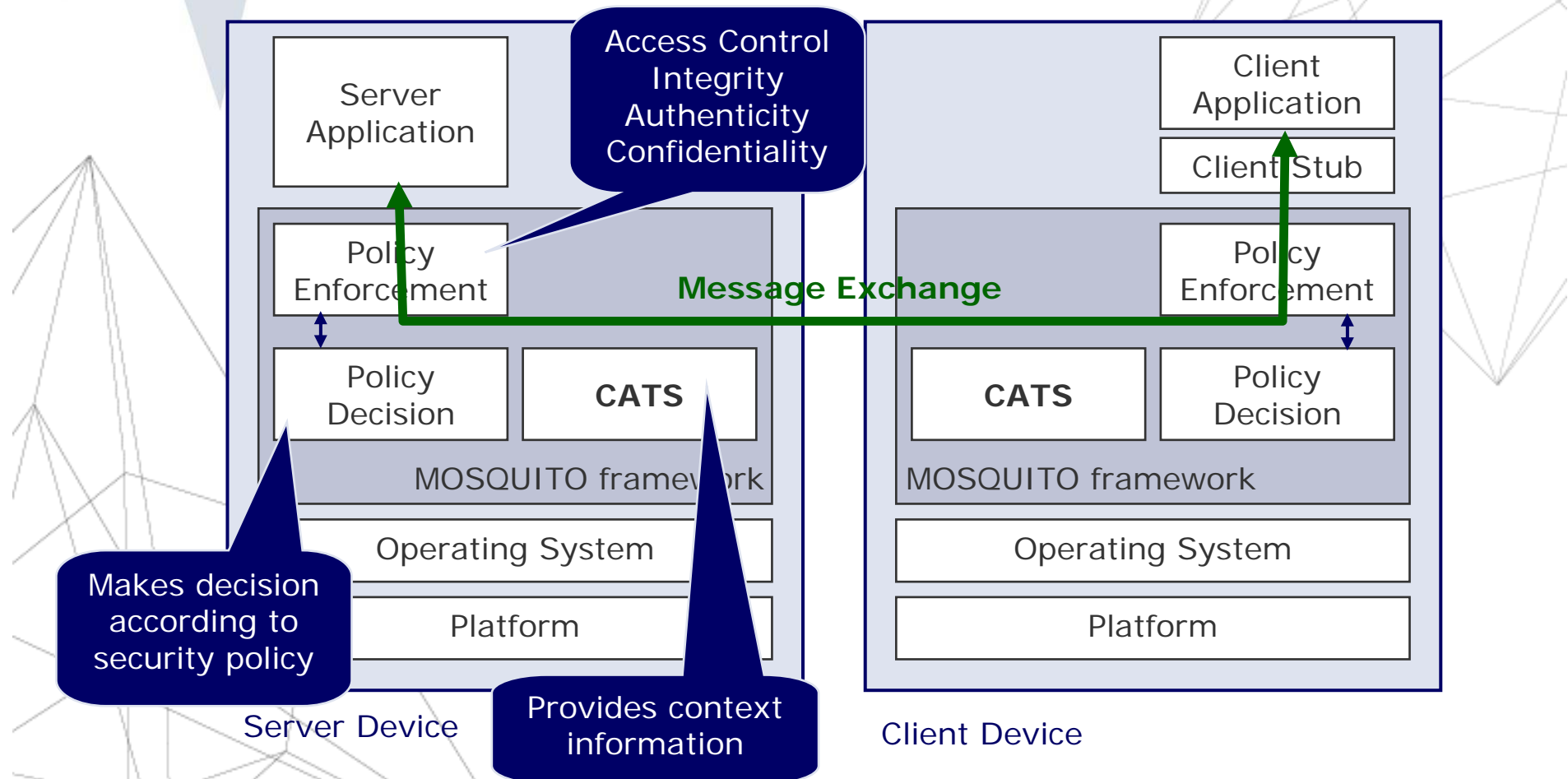
- CATS architecture development **Almost done**
- Define context-aware security policy **In progress**
- Design and implement trusted context information service provider (TCISP) **Partner**
- Implement CATS components **In progress**

Publications

- Sven Lachmund, Frank Fransen, Eddy Olk: Context-Awareness, Security and Trust, Invited paper, WPMC05, September 18-22, 2005, Aalborg, Denmark

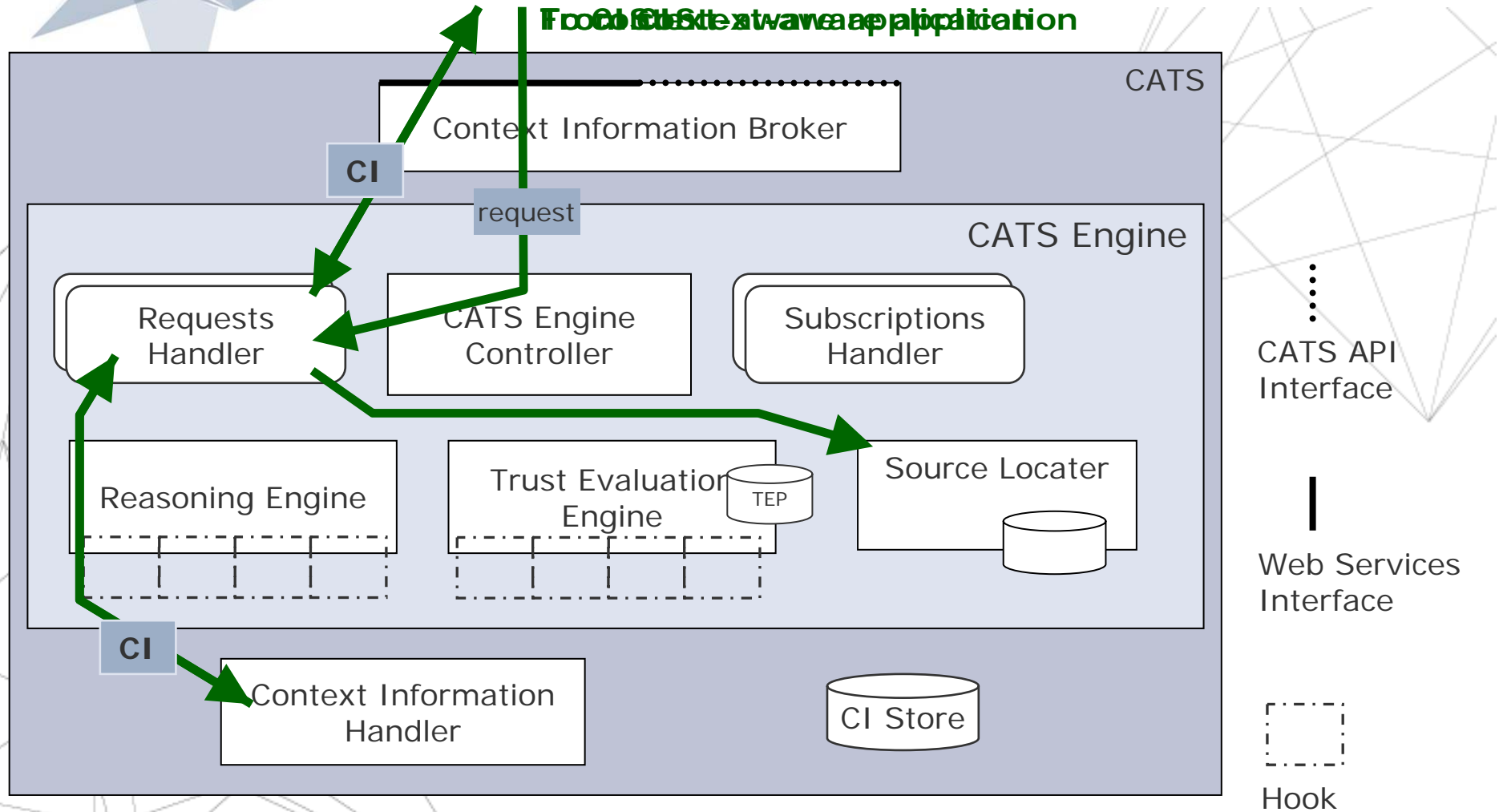
- 
- 
- Ubiquitous computing will increase variety and amount of communicating devices
 - Ubiquitous computing increases need for configuration → Context-awareness can be used to decrease user's involvement
 - Context-awareness enables auto-configuration
 - Auto-configuration should include security-relevant configuration as well
 - A MNO can implement trusted CIS as service for its customers
 - Handsets can make use of CI provided by MNO's trusted CIS
 - CATS can be implemented on handsets

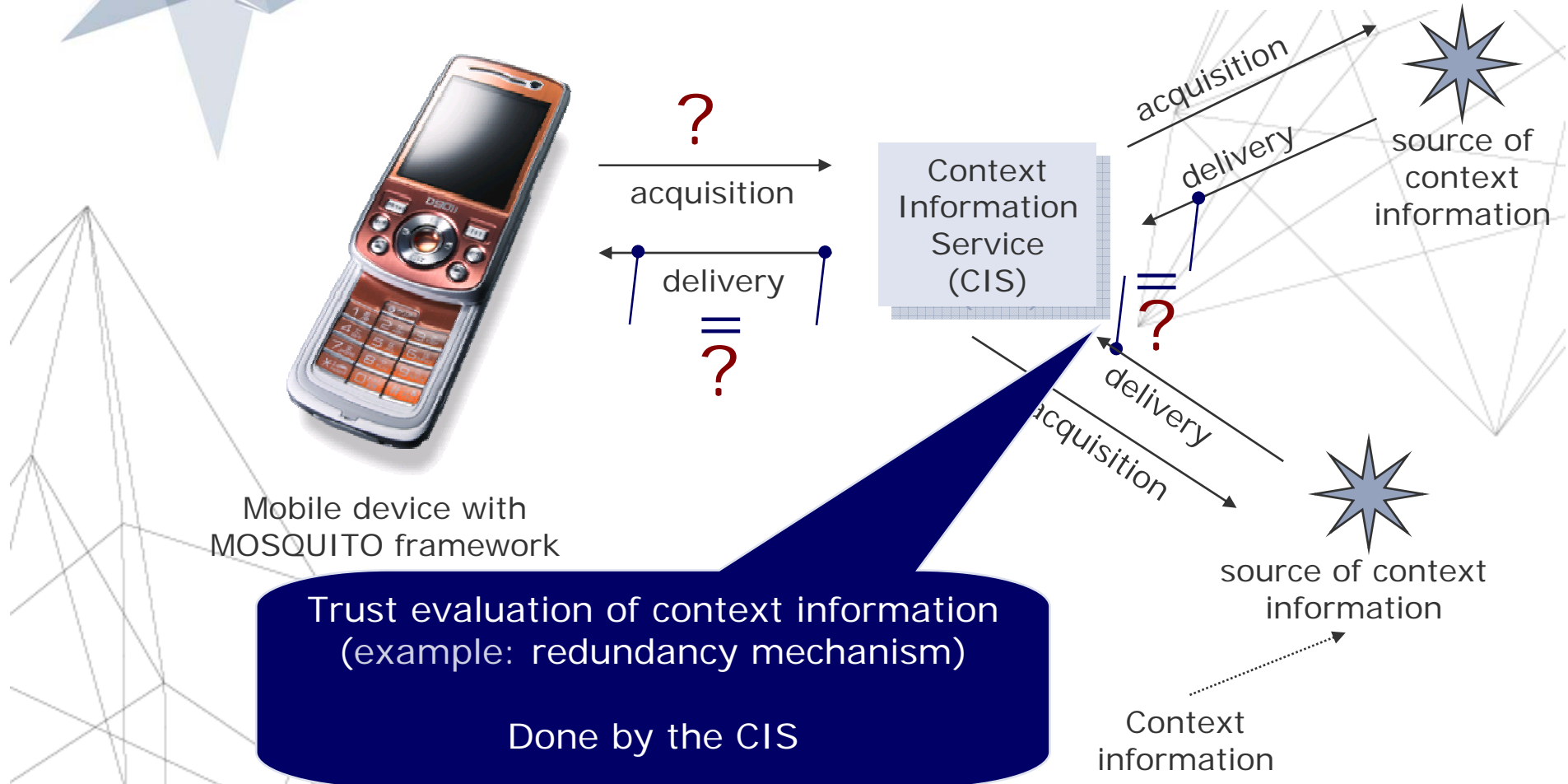
- 
- Context-Aware Trust and Security (CATS)
 - Central point for applications to acquire CI
 - performs trust evaluation of CI and CIS
 - Gain confidence in CI representing actual context
 - Establish trust relationship with CISP
 - Contains trust evaluation mechanisms
 - Trust evaluation is controlled by policies
 - Benefits
 - Enables applications to make security-relevant decisions based on trusted CI
 - Supports auto-configuration with low user involvement
 - Keeps functional logic of acquisition and trust evaluation of CI out of the application




CATS = Context-Aware Trust and Security

CATS Engine Architecture Overview





- Trust evaluation makes trusted CI out of CI



IST-Directorate General / Integrating and strengthening the ERA. The project MOSQUITO is supported by the European Community. This document does not represent the opinion of the European Community. It is also the sole responsibility of the author and not the responsibility of the European Community using any data that might appear therein.