RUHR-UNIVERSITÄT BOCHUM

RUB

Sometimes it's better to be STUCK!

SAML Transportation Unit for Cryptographic Keys

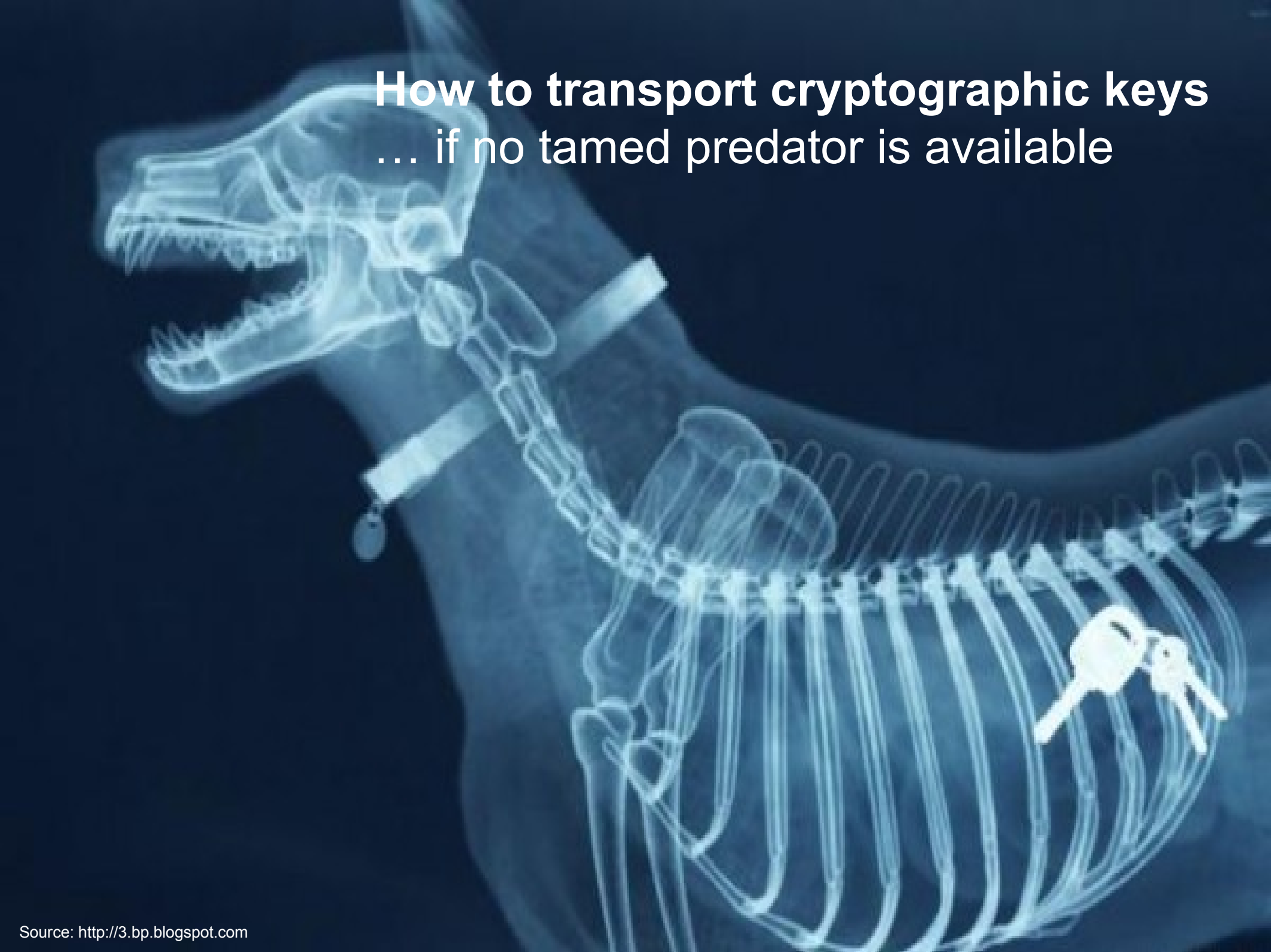
28.11.2012

Horst Görtz Institute for IT-Security
Chair for Network and Data Security

Source: http://3.bp.blogspot.com

How to transport cryptographic keys

… if no tamed predator is available



Source: http://3.bp.blogspot.com

Why transport key material?

Why transport key material?

- Web Crypto API

  "JavaScript API for performing basic cryptographic operations in web applications"

Why transport key material?

- Web Crypto API

  "JavaScript API for performing basic cryptographic operations in web applications"

- Authenticated Key Exchange

Why transport key material?

- Web Crypto API

  "JavaScript API for performing basic cryptographic operations in web applications"

- Authenticated Key Exchange
- Combining Identity Management/Federation and Key Exchange

Why choose SAML for key transport?

Why choose SAML for key transport?

- SAML

  "Security Assertion Markup Language"

Why choose SAML for key transport?

- SAML

  "Security Assertion Markup Language"

- Standard for exchanging security statements (**`Assertion`**s) about subjects

  Authentication / Authorization / Attestation / …

Why choose SAML for key transport?

- SAML

  "Security Assertion Markup Language"

- Standard for exchanging security statements (**`Assertion`**s) about subjects

  Authentication / Authorization / Attestation / …

- XML-based

Why choose SAML for key transport?

- SAML

  "Security Assertion Markup Language"
- Standard for exchanging security statements (**`Assertions`**) about subjects

  Authentication / Authorization / Attestation / …
- XML-based
- Flexible, extensive, **extensible**

Why choose SAML for key transport?

- SAML

  "Security Assertion Markup Language"
- Standard for exchanging security statements (**`Assertions`**) about subjects

  Authentication / Authorization / Attestation / …
- XML-based
- Flexible, extensive, **extensible**
- Most known usage scenario: Single-Sign-On

Advantages of the proposal

Build upon approved technologies

Advantages of the proposal

Build upon approved technologies

- SAML

Advantages of the proposal

Build upon approved technologies

- SAML
- XML

Advantages of the proposal

Build upon approved technologies

- SAML
- XML
- XML Encryption

Advantages of the proposal

Build upon approved technologies

- SAML
- XML
- XML Encryption
- XML Signature

Advantages of the proposal

Seamless integration

Advantages of the proposal
Seamless integration

- Usage of standard SAML Extension Points

Advantages of the proposal
Seamless integration

- Usage of standard SAML Extension Points
- No Schema violation

Advantages of the proposal
Seamless integration

- Usage of standard SAML Extension Points
- No Schema violation
- Fully SAML compatible

Advantages of the proposal
Binding keys to assertions

Assertions offer support for:

Advantages of the proposal
Binding keys to assertions

Assertions offer support for:

- Integrity protection through digital signatures

Advantages of the proposal
Binding keys to assertions

Assertions offer support for:

- Integrity protection through digital signatures
- Confidentiality protection through encryption

Advantages of the proposal
Binding keys to assertions

Assertions offer support for:

- Integrity protection through digital signatures
- Confidentiality protection through encryption
- Time-bound validity

Advantages of the proposal
Binding keys to assertions

Assertions offer support for:

- Integrity protection through digital signatures
- Confidentiality protection through encryption
- Time-bound validity
- Detailed issuer and subject information

Advantages of the proposal
Binding keys to assertions

Assertions offer support for:

- Integrity protection through digital signatures
- Confidentiality protection through encryption
- Time-bound validity
- Detailed issuer and subject information
- Identity binding

Advantages of the proposal
Identity and Key federation

Advantages of the proposal
Identity and Key federation

- Key federation between multiple services

Advantages of the proposal
Identity and Key federation

- Key federation between multiple services
- Inseparable Identity – Key Binding, beyond service borders

Advantages of the proposal

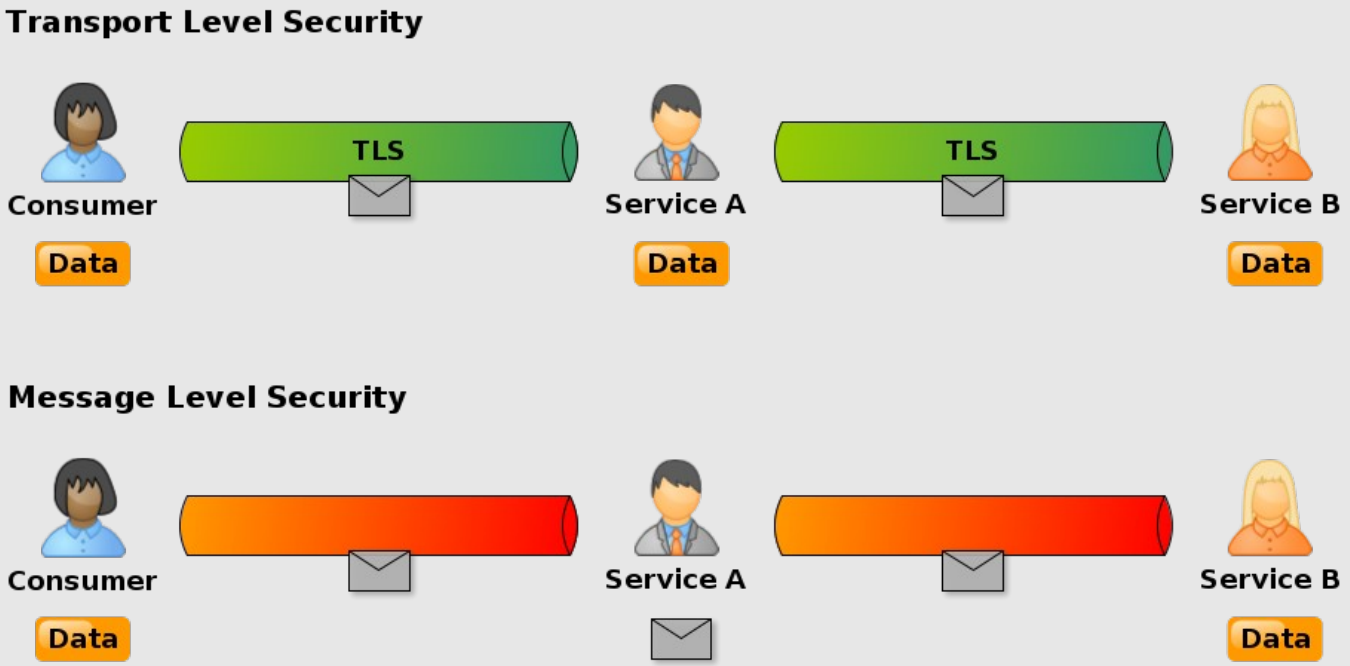
Message level security

Advantages of the proposal
Message level security

- Security at message level

Advantages of the proposal
Message level security

- Security at message level



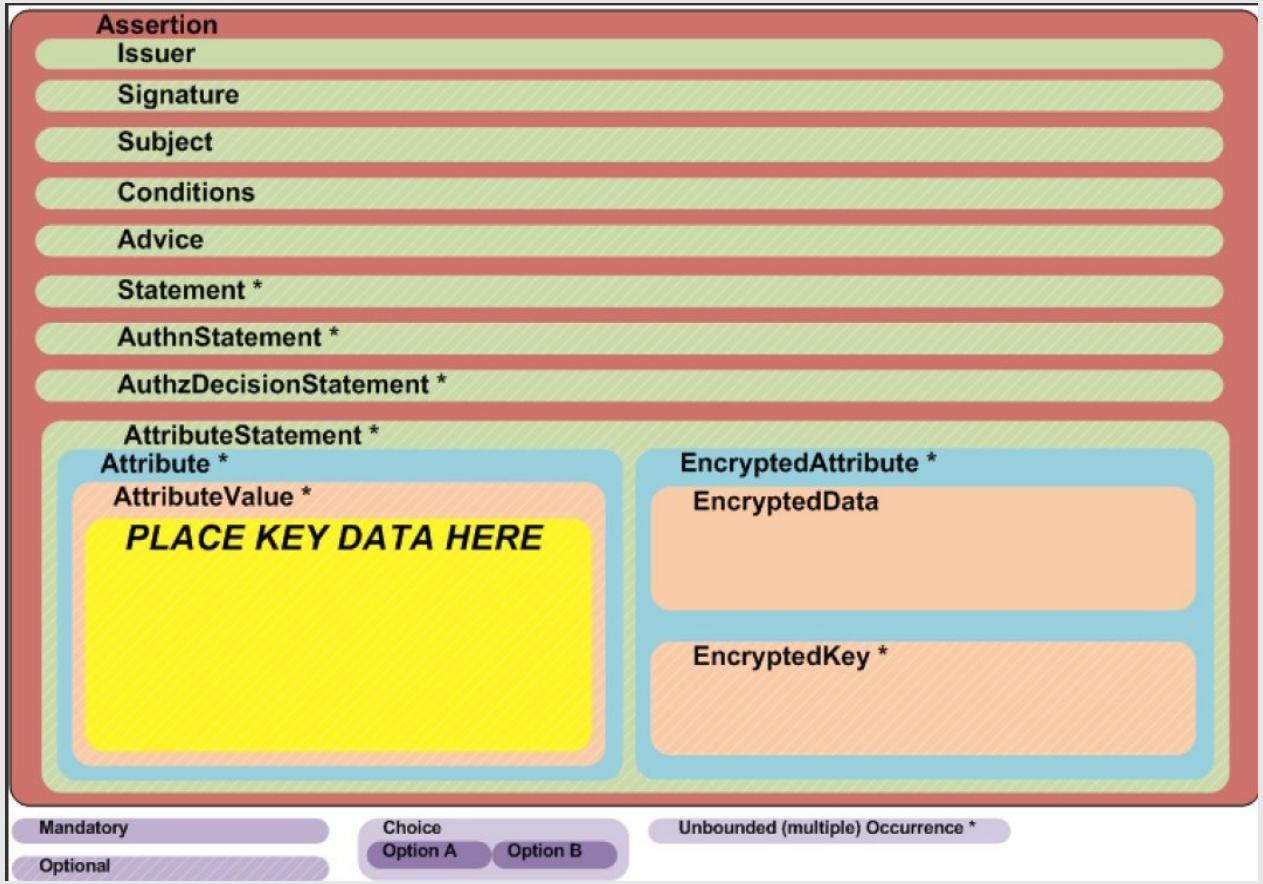
STUCK

STUCK

`Assertion` structure

STUCK

Assertion structure

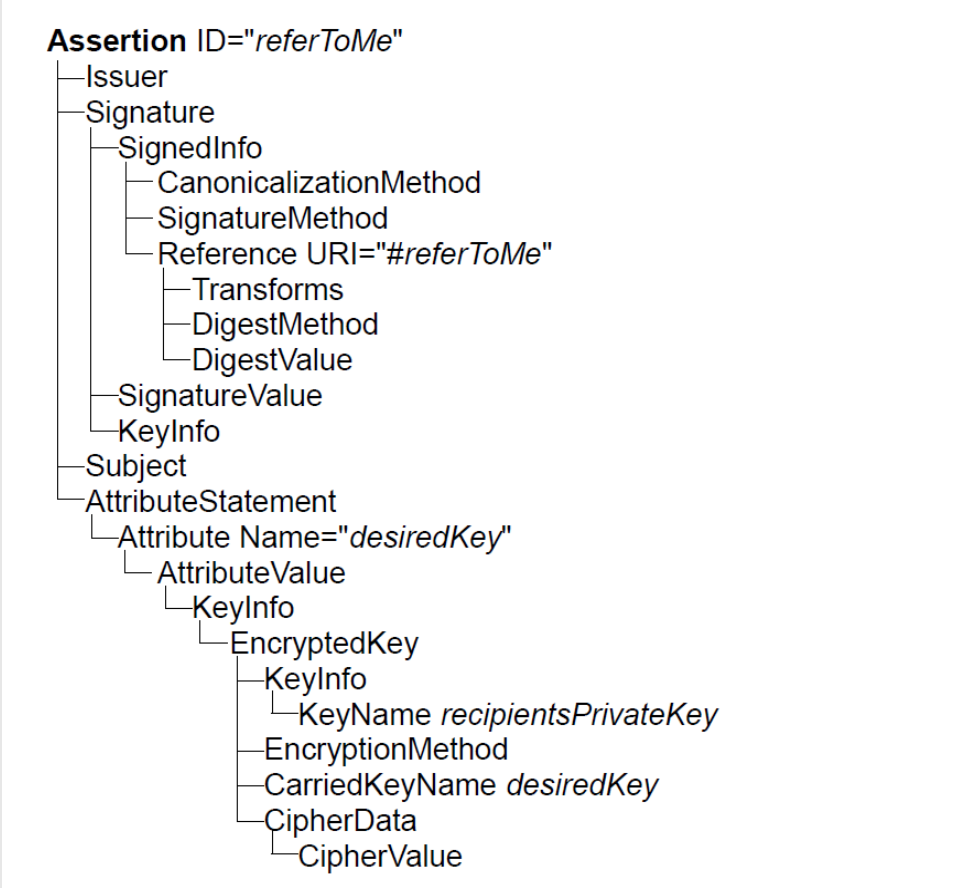


STUCK

Proposal: Proof-of-concept `Assertion`

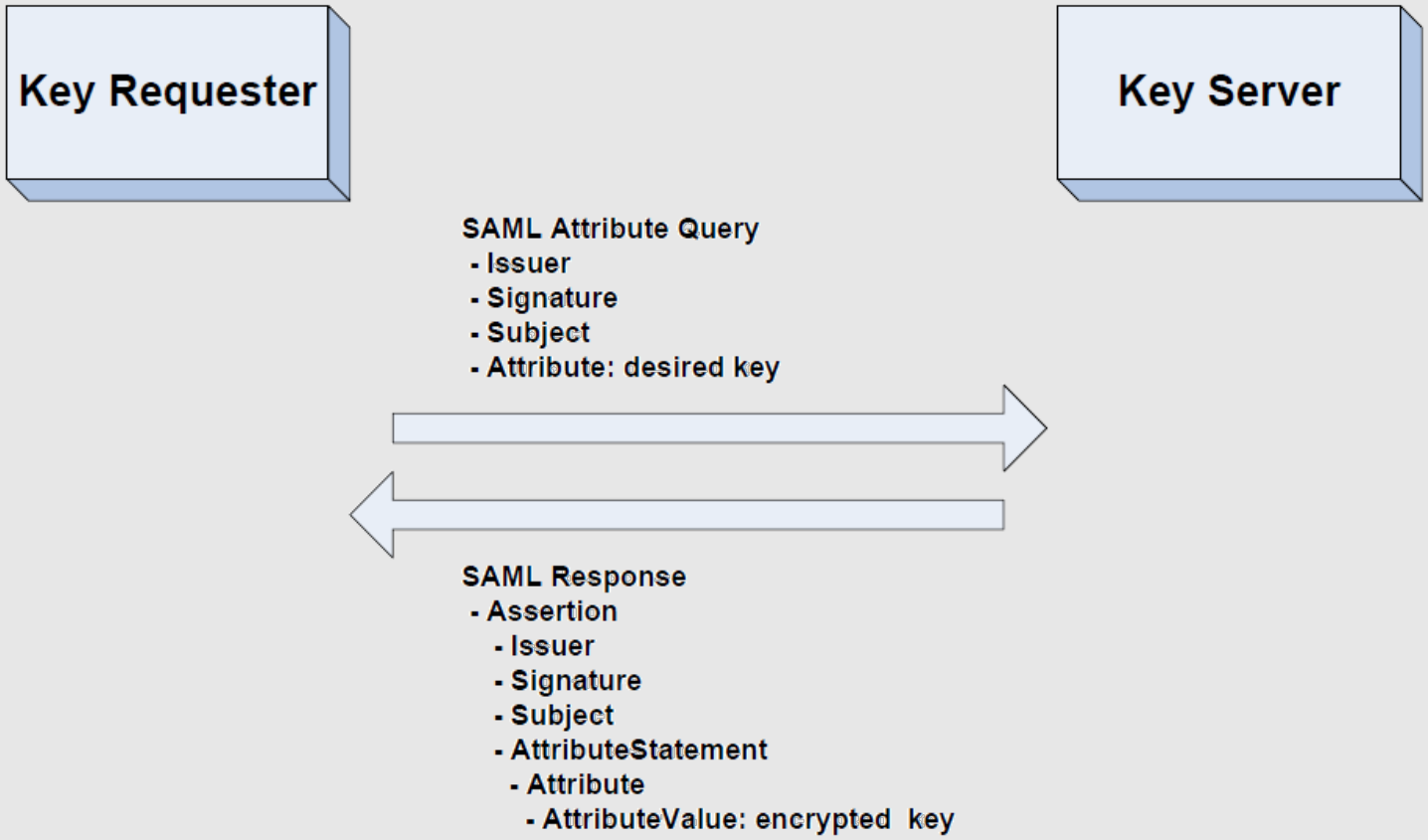
STUCK

Proposal: Proof-of-concept `Assertion`

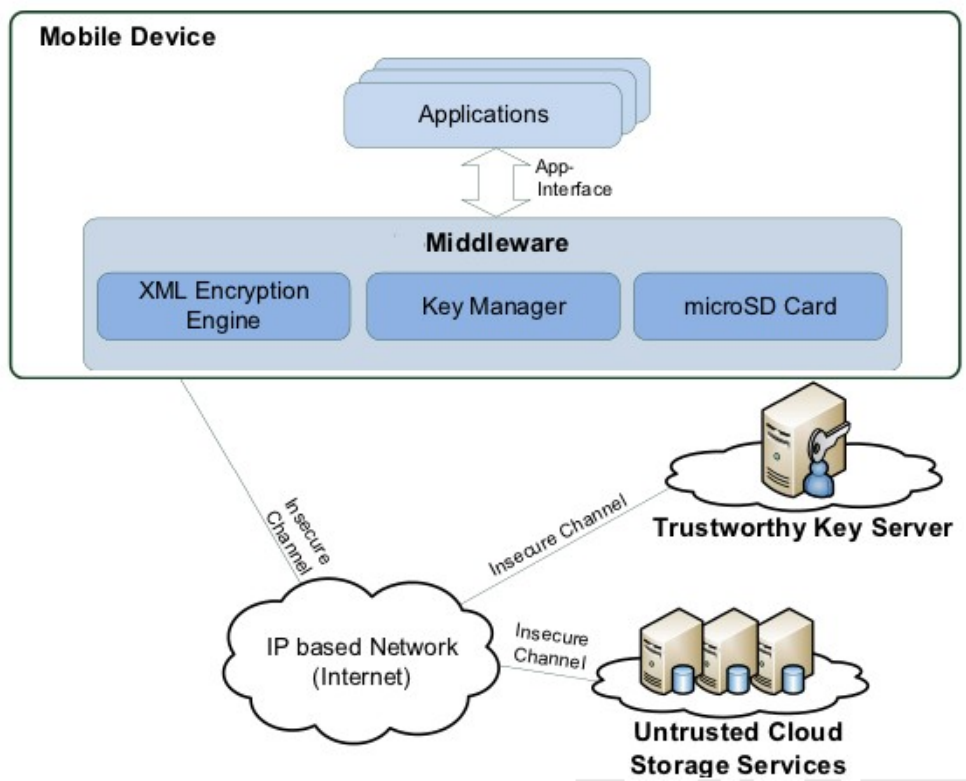


STUCK

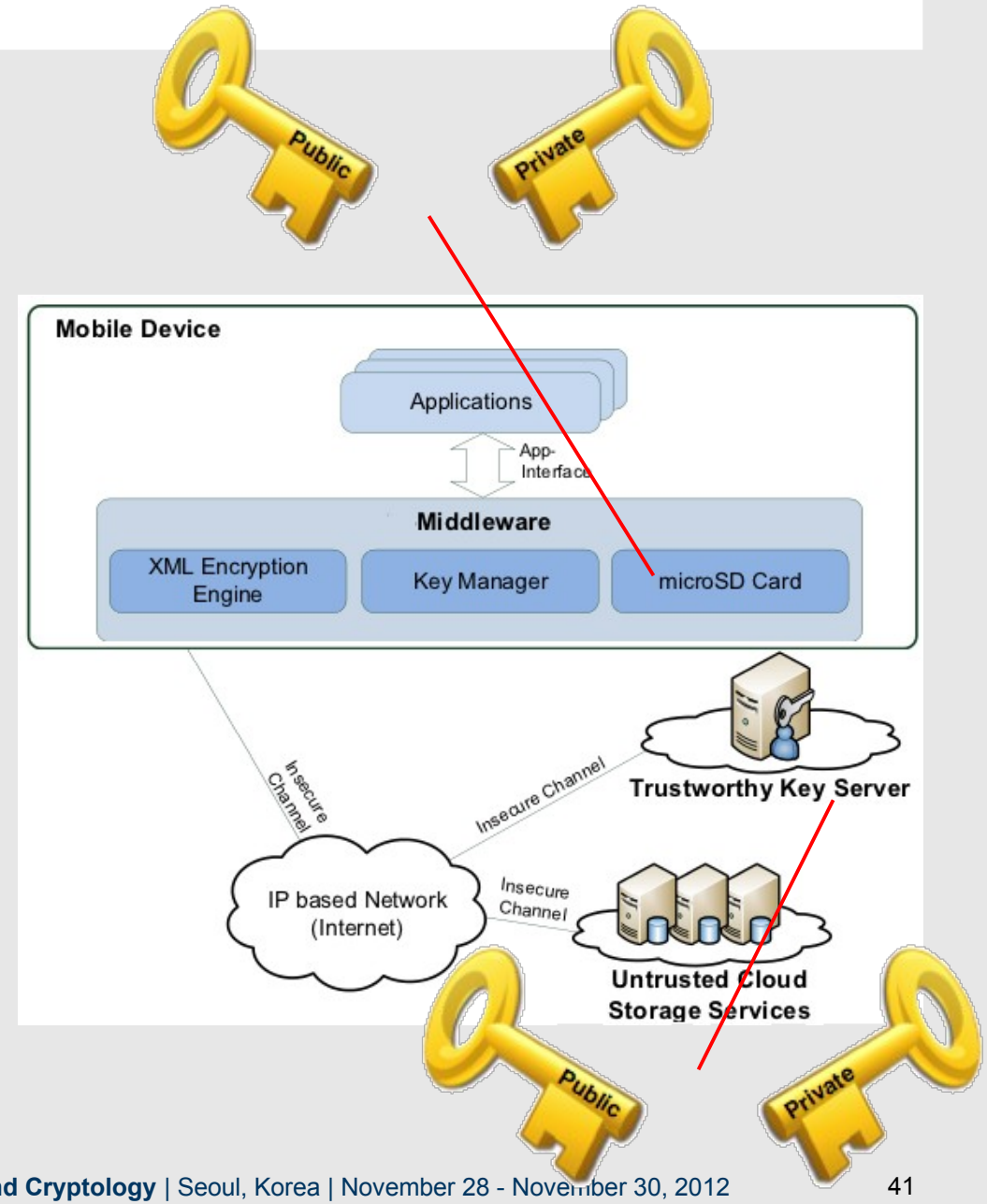
Proposal: Compatibility with SAML Protocols



Case study
Sec² research project

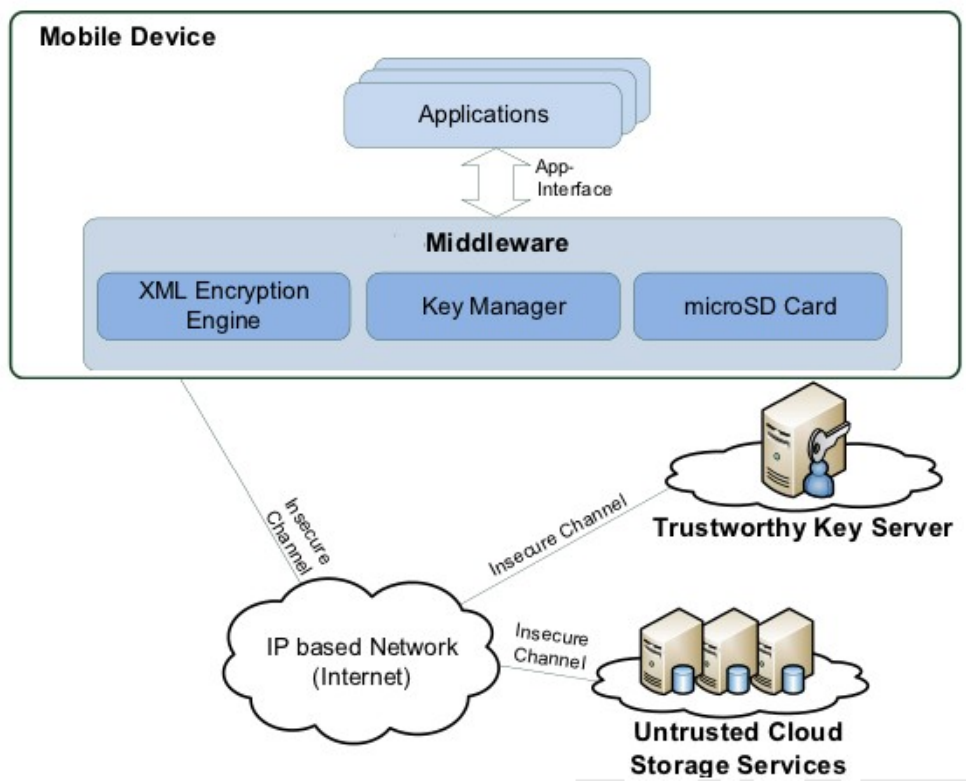


Case study
Sec² research project



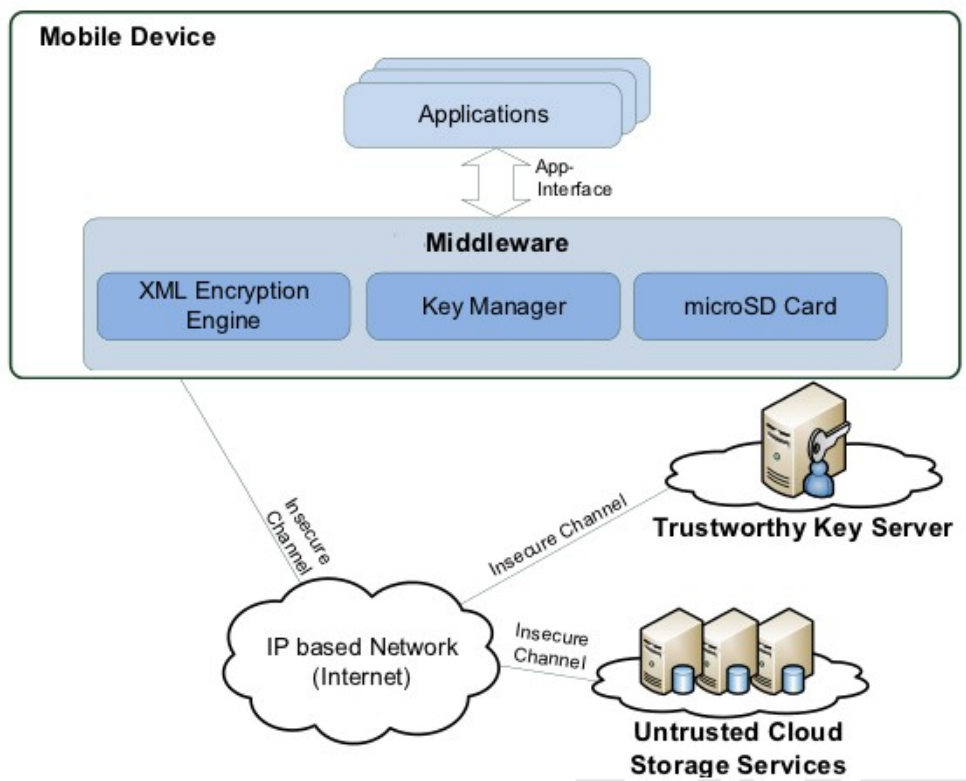
Case study
Sec² research project

1. Middleware fetches (encrypted) data from untrusted Cloud storage



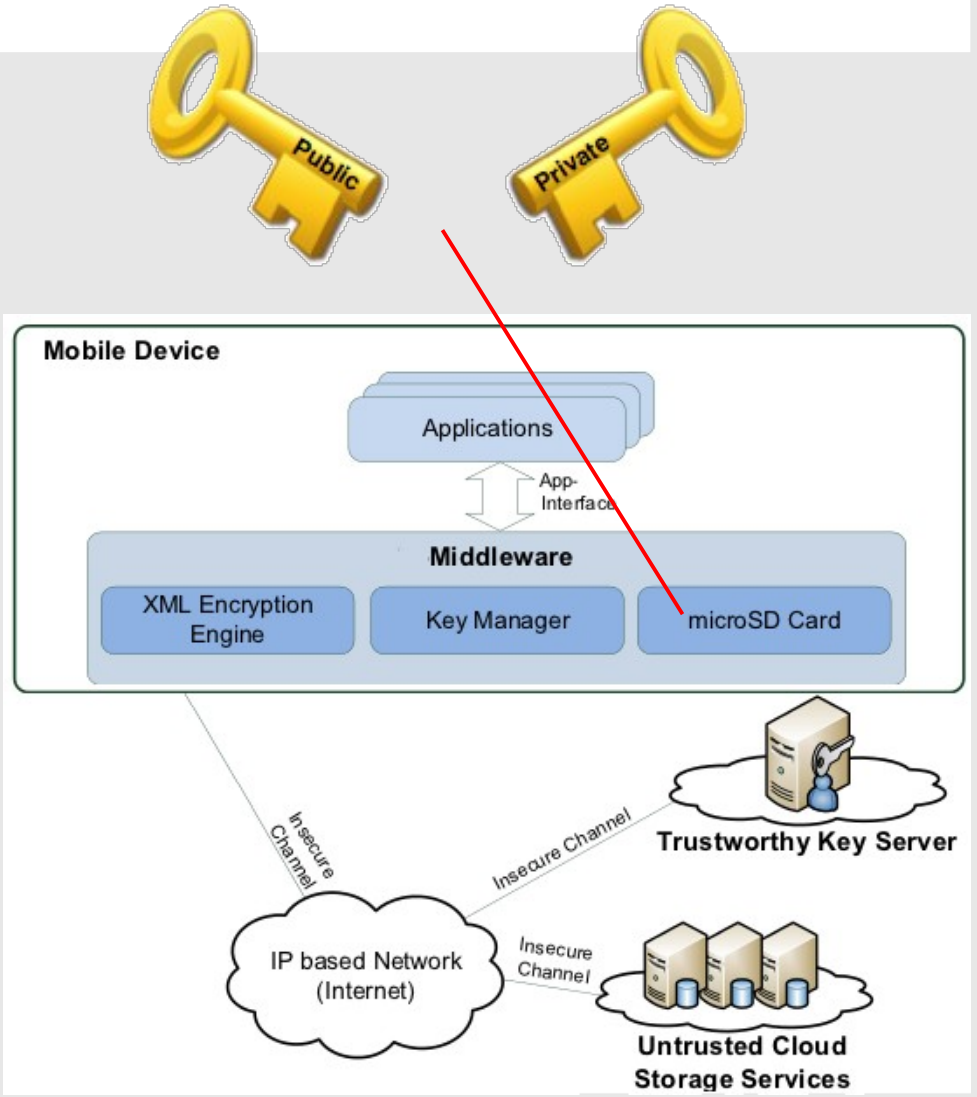
Case study
Sec² research project

1. Middleware fetches (encrypted) data from untrusted Cloud storage
2. MicroSD not in posession of required key (yet)



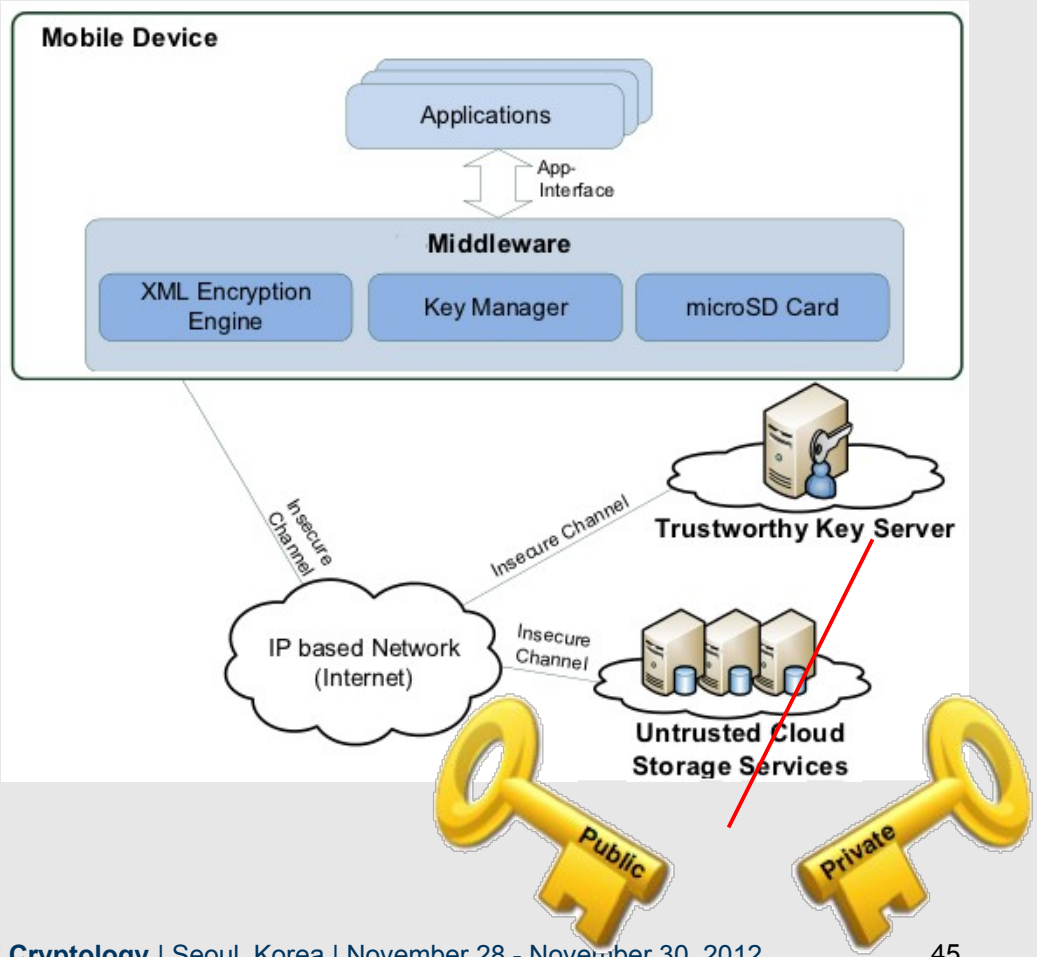
Case study
Sec² research project

1. Middleware fetches (encrypted) data from untrusted Cloud storage
2. MicroSD not in posession of required key (yet)
3. Key is requested with SAML AttributeQuery (including signed authorization data)



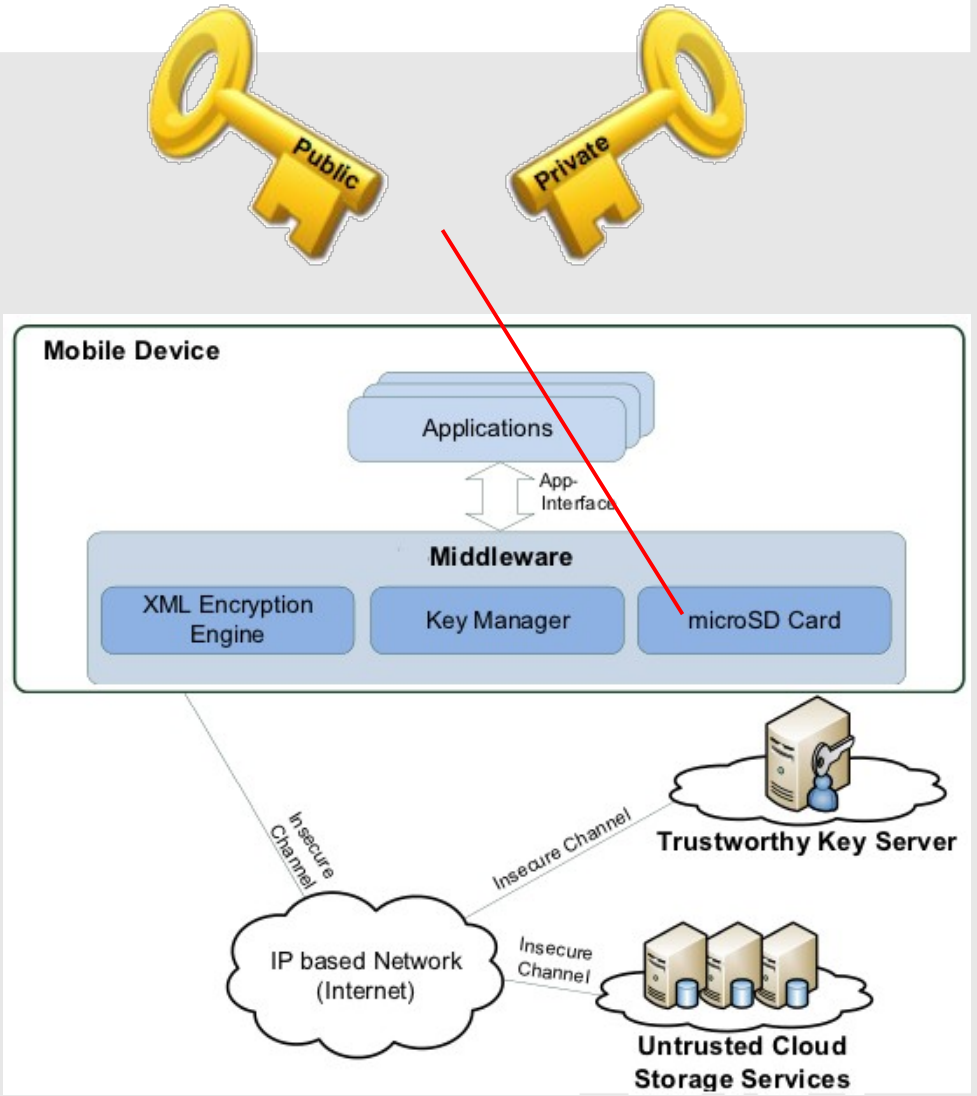
Case study
Sec² research project

1. Middleware fetches (encrypted) data from untrusted Cloud storage
2. MicroSD not in posession of required key (yet)
3. Key is requested with SAML AttributeQuery (including signed authorization data)
4. Key Server responds with signed and encrypted key



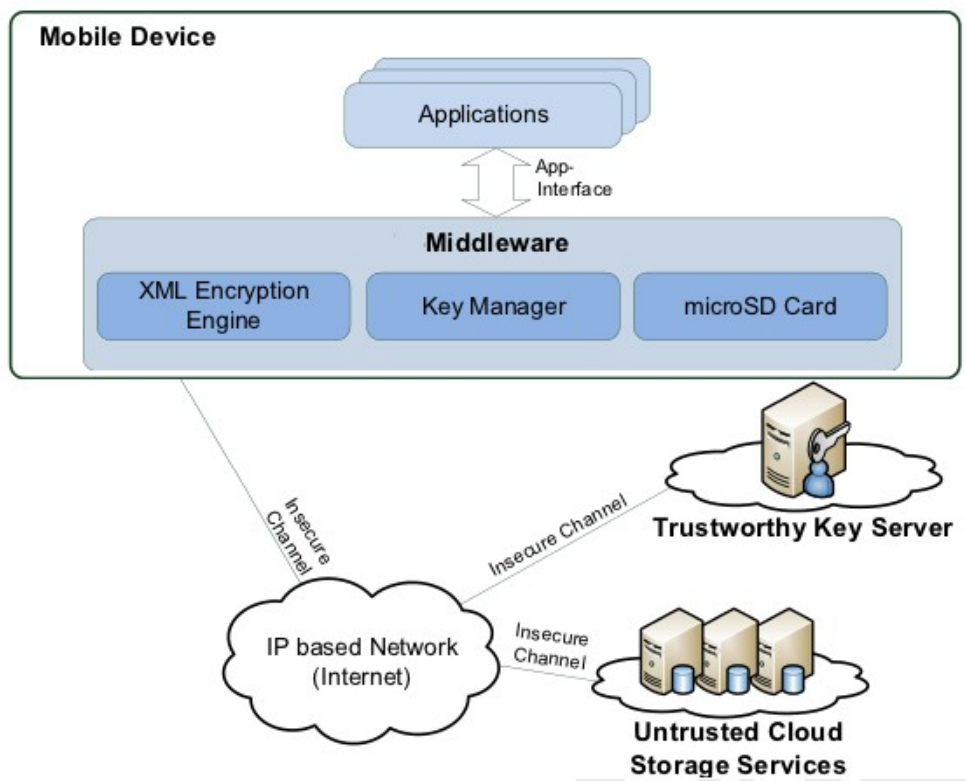
Case study
Sec² research project

1. Middleware fetches (encrypted) data from untrusted Cloud storage
2. MicroSD not in posession of required key (yet)
3. Key is requested with SAML AttributeQuery (including signed authorization data)
4. Key Server responds with signed and encrypted key
5. MicroSD decrypts wrapped key



Case study
Sec² research project

1. Middleware fetches (encrypted) data from untrusted Cloud storage
2. MicroSD not in posession of required key (yet)
3. Key is requested with SAML AttributeQuery (including signed authorization data)
4. Key Server responds with signed and encrypted key
5. MicroSD decrypts wrapped key
6. Middleware decrypts fetched data



Time for questions

Source:http://www.rhodius-mineralwasser.de

Christopher Meyer
christopher.meyer@rub.de
http://armoredbarista.blogspot.com
http://www.nds.rub.de