RUB

Sec^2 SECURE MOBILE SOLUTION FOR DISTRIBUTED PUBLIC CLOUD STORAGES

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

2nd International Conference on Cloud Computing and Services Science, **CLOSER 2012**

19.04.2012 Porto, Portugal

Christopher Meyer
christopher.meyer@rub.de
www.nds.rub.de

Motivation
Risks of Cloud Storage

GOVERNMENT CLOUD, TECHNOLOGY

EXPERTS BELIEVE CLOUD COMPUTING INCREASES RISK OF DATA LEAKAGE

By Alice Kok | 22 October 2008

Cloud computing has been illuminated as being thoug ... decrease the risk of data leakage. A recent symposium on the topi ... 's key finding in its post symposium survey: the attendees ... computing increases, not decreases the risk of da

This latest form of outsourcing IT services and ... delivery of these services over the internet is ... key business driver for the next generation ... companies as well as for large establishe

By leveraging the established and out ... infrastructure of cloud computing ser ... closely related technologies such a ... Service (SaaS) and virtualisation ... sizes now have the ability to ad ... complex services efficiently ar ... unprecedented speed.

Surprising to note is that ... over 60 experts from bo ... held a prior vote wher ... the Information Syst ... members was exp ... made secu

Microsoft Cloud Data Breach Heralds Things to Come

By Kelly Thomas, PCWorld

What might be the first major cloud data ... that data contained within its Business ... by non-authorized users.

SIMILAR ARTICLES

CLOUD COMPUTING REMAINS CONTROVERSIAL

Dropbox lets anyone log in as anyone - so check your files now!

Hi there! If you're new here, you might want to subscribe to the RSS feed for updates.

by Paul Ducklin on June 21, 2011 | Comments (7)

FILED UNDER: Data loss, Privacy

... cloud-based file storing-and-sharing ... should check on the data they've ... following the company's ... access controls for

LastPass Possibly Hacked, Cloud Security Concerns on the Rise

by KIRIL ON MAY 5, 2011 AT 11:08 AM in BACKUPS, BUSINESS, CLOUD COMPUTING, COMPANIES, COM ... CONTRIBUTORS, NEWS, SECURITY, STORAGE, TECHNOLOGY

LastPass Possibly Hacked, Cloud Security Concerns on the Rise

Conspiracy theory admirers will be happy to hear the news that today, following ... security breaches at Sony, cloud-based password storage and ... possible successful hacker's attack against its server

"If you have a strong, non-di ... brute-forcing w ...

Information Leakage in Cloud Computing

Published: 2009-09-13, Updated: 2009-09-13 08:58:33 UTC (Version: 1)

Home / News & Blogs / ZDNet Government

Is the cloud still safe? How to survive a cloud computing disaster.

By David Gewirtz | May 15, 2011, 5:00am PDT

Summary: The news isn't just limited to ... been cloud failures at ...

... last week discussing ways ... and discovery of info ... ng that this alone ... d about as more ... a high likelihood t

Sources:
[isc.sans.edu, www.cloudtweaks.com, nakedsecurity.sophos.com, www.infoworld.com, www.hgi.rub.de, www.zdnet.com, www.futuregov.asia, www.pcworld.com]

Cloud Storage Security

Status Quo

Cloud Storage Security

Status Quo

- No encryption

Cloud Storage Security

Status Quo

- No encryption
- Provider based encryption

Cloud Storage Security

Status Quo

- No encryption
- Provider based encryption
- User based encryption with desktop tools (Truecrypt, GPG, ...)

Cloud Storage Security

Status which would be desirable

Cloud Storage Security

Status which would be desirable

- Secure storage of user supplied data on any cloud storage

Cloud Storage Security

Status which would be desirable

- Secure storage of user supplied data on any cloud storage
- Group communication and collaboration capabilities

Cloud Storage Security

Status which would be desirable

- Secure storage of user supplied data on any cloud storage
- Group communication and collaboration capabilities
- Complete control over data by group participants / particular users

Cloud Storage Security

Status which would be desirable

- Secure storage of user supplied data on any cloud storage
- Group communication and collaboration capabilities
- Complete control over data by group participants / particular users
- No trust relationships between user and cloud storage provider

Sec² Concept

Major Design Goals

Sec² Concept

Major Design Goals

- User controlled security
  - - Users keep control over their data

Sec² Concept

Major Design Goals

- User controlled security
  - Users keep control over their data
- Scalability
  - Extensible, modular and interoperable architecture

Sec² Concept

Major Design Goals

- User controlled security
  - Users keep control over their data
- Scalability
  - Extensible, modular and interoperable architecture
- Efficiency
  - Hardware accelerated and optimized crypto algorithms

Sec² Concept

Major Design Goals

- User controlled security
  - Users keep control over their data
- Scalability
  - Extensible, modular and interoperable architecture
- Efficiency
  - Hardware accelerated and optimized crypto algorithms
- Mobility
  - Specially designed for mobile devices

Sec² Concept

Major Design Goals

- User controlled security
  - Users keep control over their data
- Scalability
  - Extensible, modular and interoperable architecture
- Efficiency
  - Hardware accelerated and optimized crypto algorithms
- Mobility
  - Specially designed for mobile devices
- Transpareny
  - As transparent as possible for end-users

Sec² Concept

Major Design Goals

- User controlled security
  - Users keep control over their data
- Scalability
  - Extensible, modular and interoperable architecture
- Efficiency
  - Hardware accelerated and optimized crypto algorithms
- Mobility
  - Specially designed for mobile devices
- Transpareny
  - As transparent as possible for end-users
- Seamless integration
  - Easy to integrate in existing systems

Sec² Concept

Major Design Goals

- User controlled security
  - Users keep control over their data
- Scalability
  - Extensible, modular and interoperable architecture
- Efficiency
  - Hardware accelerated and optimized crypto algorithms
- Mobility
  - Specially designed for mobile devices
- Transparency
  - As transparent as possible for end-users
- Seamless integration
  - Easy to integrate in existing systems
- Hybrid Documents
  - Partly encrypted documents with unencrypted public blocks

Sec² Concept

Aimed Security and Usability Goals

Sec² Concept

Aimed Security and Usability Goals

- Confidentiality

  - achieved by using XML Encryption

Sec² Concept
Aimed Security and Usability Goals

- Confidentiality
  - achieved by using XML Encryption
- Authenticity
  - achieved by using signed SAML Assertions

Sec² Concept

Aimed Security and Usability Goals

- Confidentiality

  - achieved by using XML Encryption
- Authenticity

  - achieved by using signed SAML Assertions
- Reliability

  - achieved by providing seamless data roaming between transport media

Sec² Concept

Aimed Security and Usability Goals

- Confidentiality

  - achieved by using XML Encryption
- Authenticity

  - achieved by using signed SAML Assertions
- Reliability

  - achieved by providing seamless data roaming between transport media
- (optional) Integrity

  - achieved by (optional) using XML Signature on payload data

Sec² Concept
Aimed Security and Usability Goals

- Confidentiality

  - achieved by using XML Encryption
- Authenticity

  - achieved by using signed SAML Assertions
- Reliability

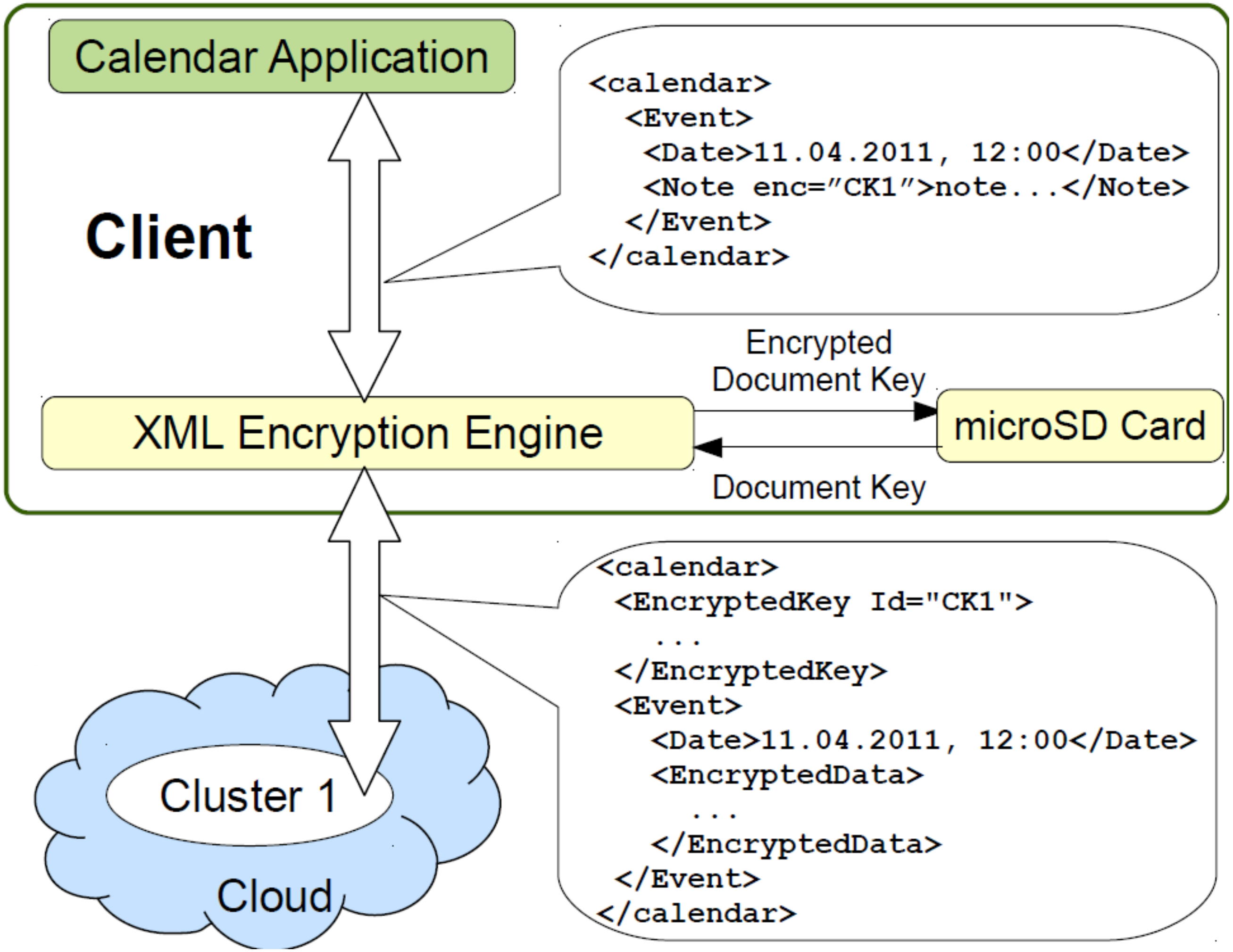
  - achieved by providing seamless data roaming between transport media
- (optional) Integrity

  - achieved by (optional) using XML Signature on payload data
- Tagging of encrypted data

  - achieved by providing unencrypted public document parts for non-confidential data

Sec^2 Concept

Example Scenario

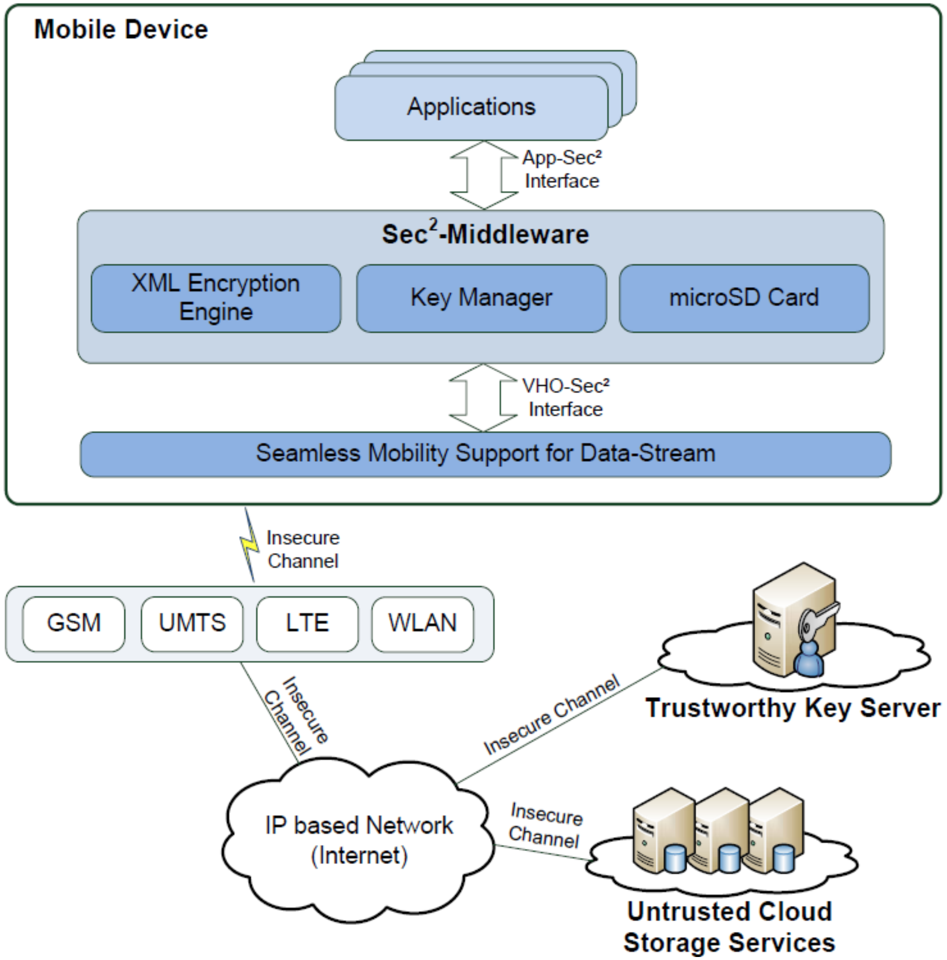


```
<calendar>
  <Event>
   <Date>11.04.2011, 12:00</Date>
   <Note enc="CK1">note...</Note>
  </Event>
</calendar>
```

```
<calendar>
  <EncryptedKey Id="CK1">
     ...
  </EncryptedKey>
  <Event>
    <Date>11.04.2011, 12:00</Date>
    <EncryptedData>
       ...
    </EncryptedData>
  </Event>
</calendar>
```

Sec² Architecture

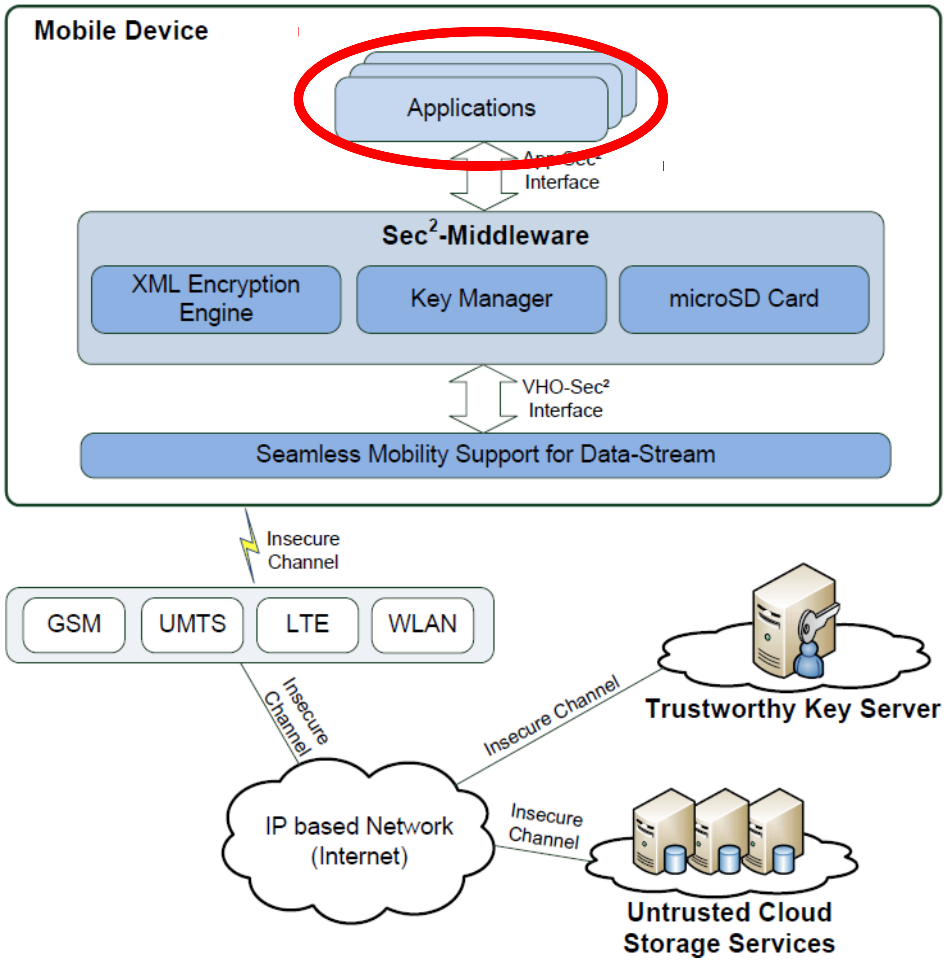
Module Scheme



Sec² Architecture

Module Scheme 1/2

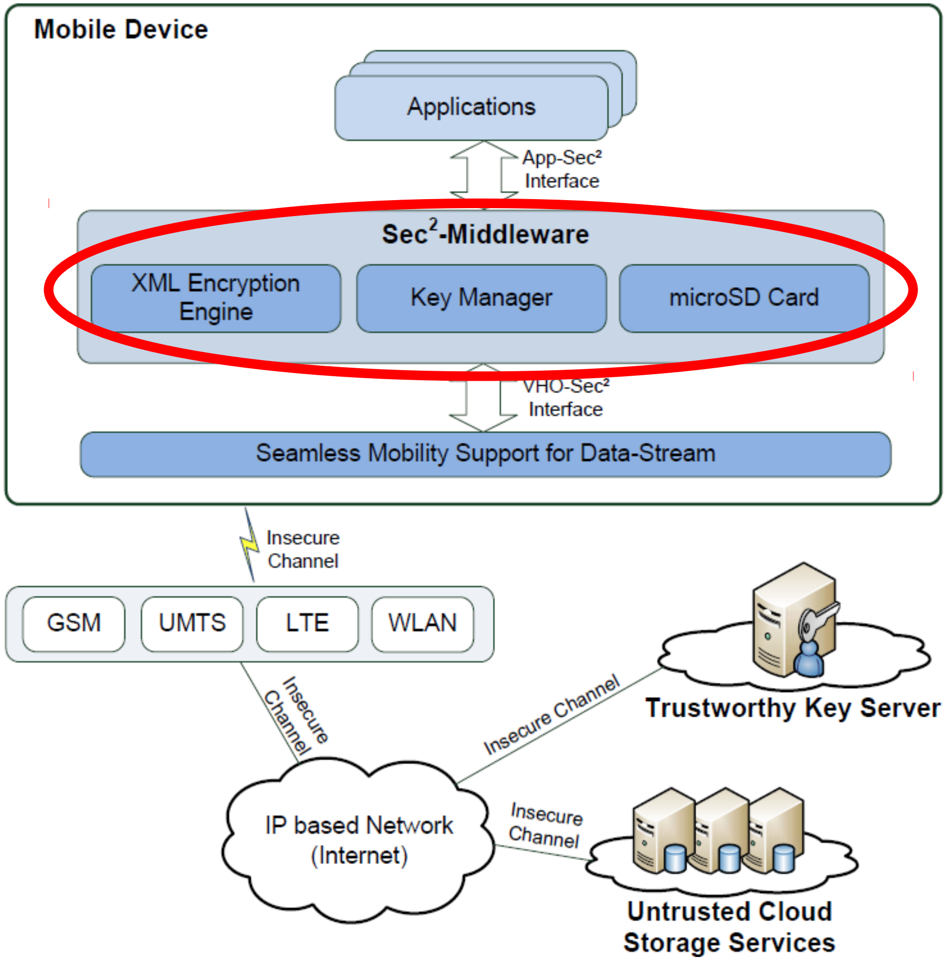
- Applications
  - End user application



Sec² Architecture

Module Scheme 1/2

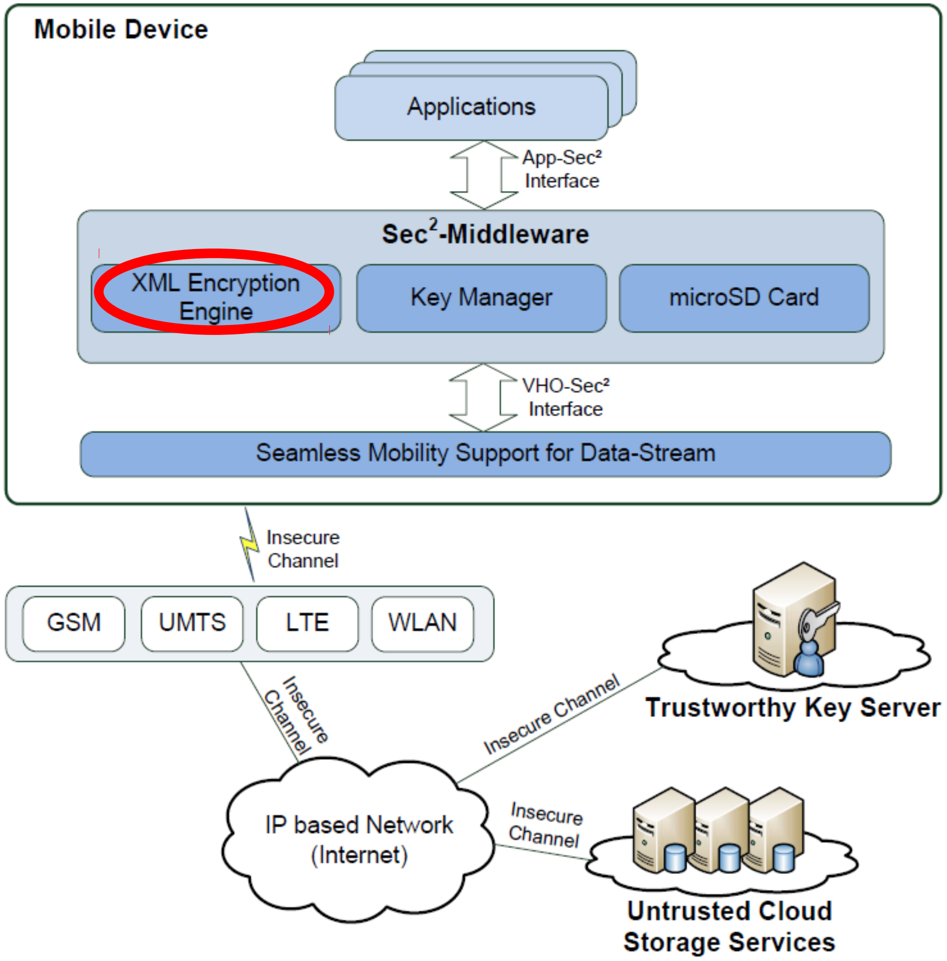
- Applications
  - End user application
- Sec² Middleware
  - Core processing



Sec² Architecture

Module Scheme 1/2

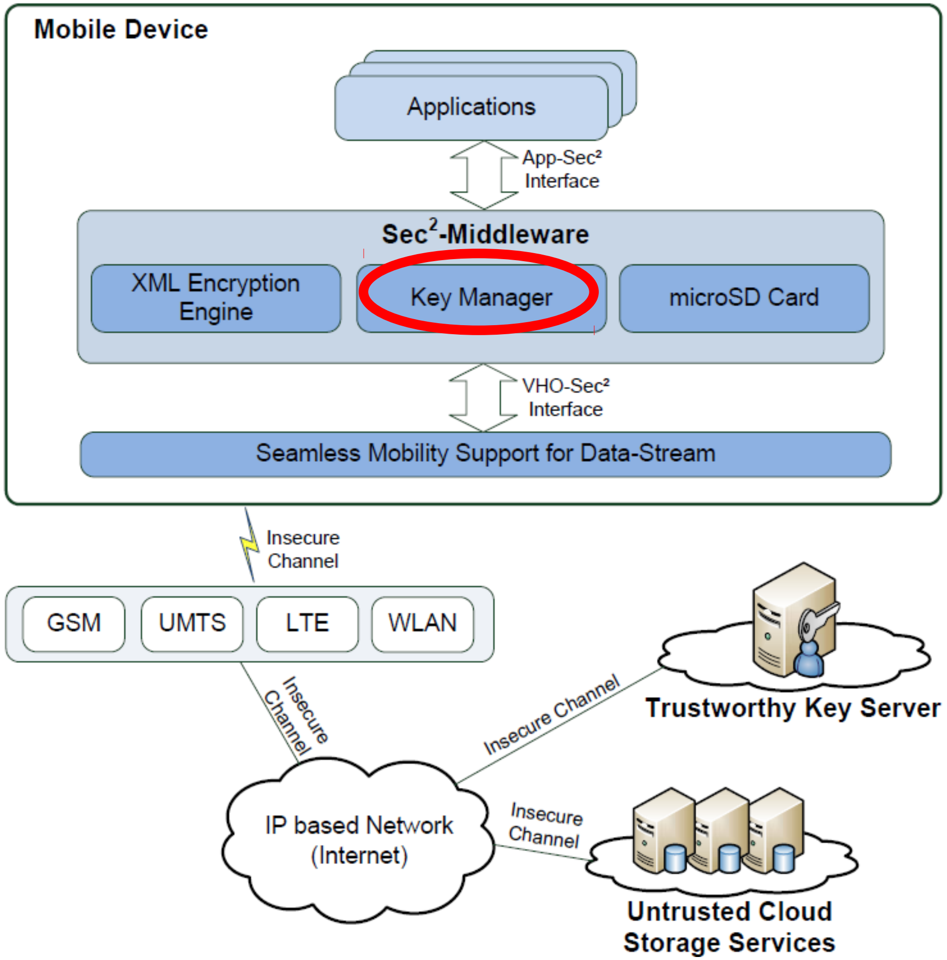
- Applications
  - End user application
- Sec² Middleware
  - Core processing
- XML Encryption Engine
  - En-/Decryption



Sec² Architecture

Module Scheme 1/2

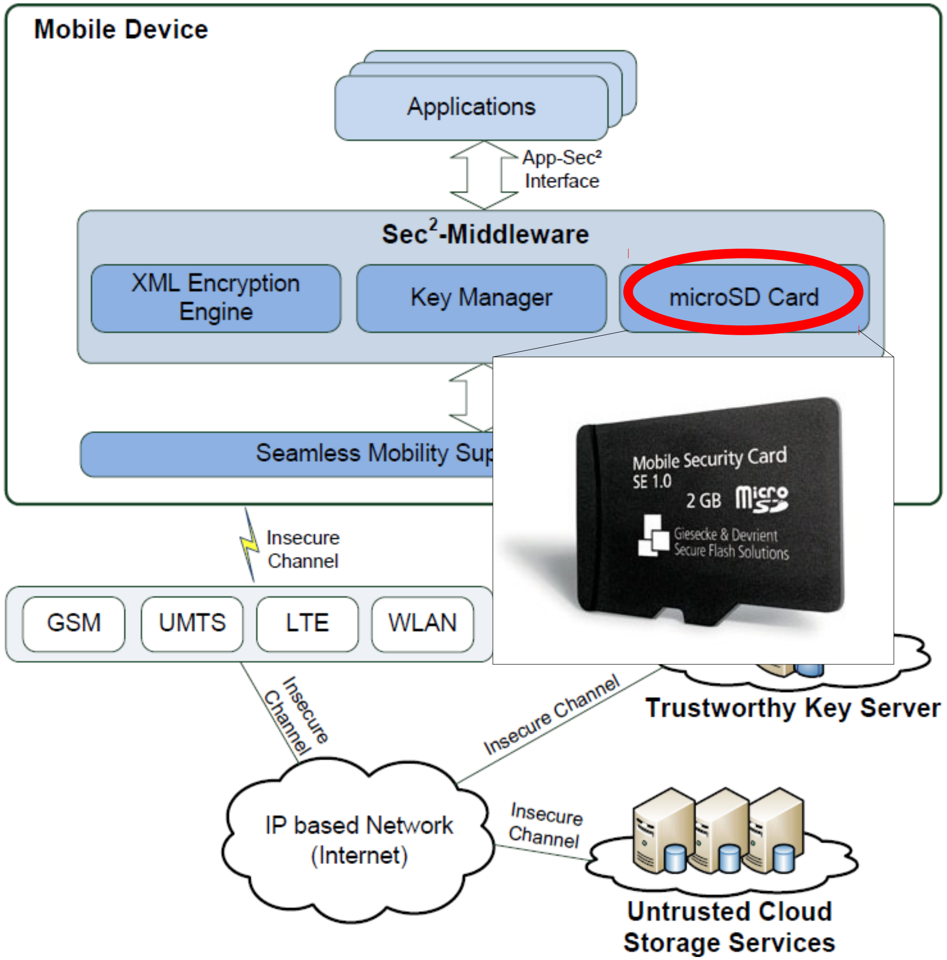
- Applications
  - End user application
- Sec² Middleware
  - Core processing
- XML Encryption Engine
  - En-/Decryption
- Key Manager
  - Key management
  - Key generation
  - Key fetching



Sec^2 Architecture

Module Scheme 1/2

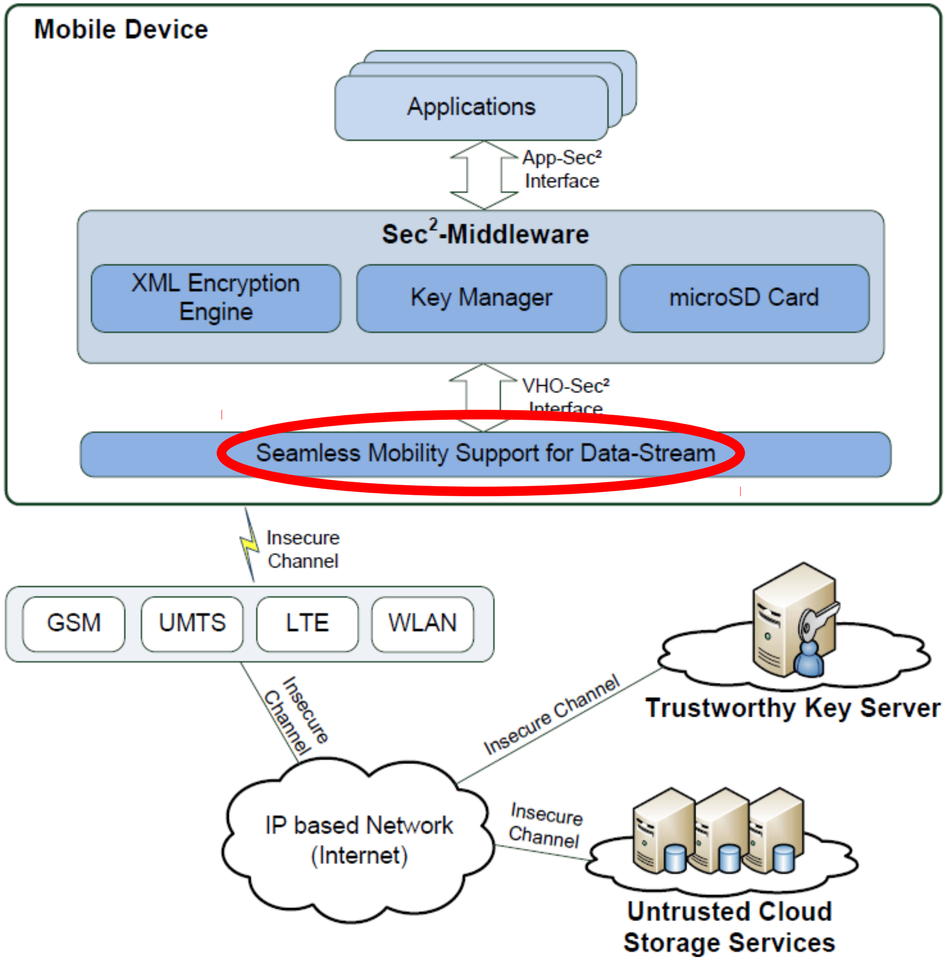
- Applications
    - End user application
- Sec^2 Middleware
    - Core processing
- XML Encryption Engine
    - XML en-/decryption
- Key Manager
    - Key management
    - Key generation
    - Key fetching
- MicroSD Card
    - Secure key storage
    - Key wrapping



Sec² Architecture

Module Scheme 2/2

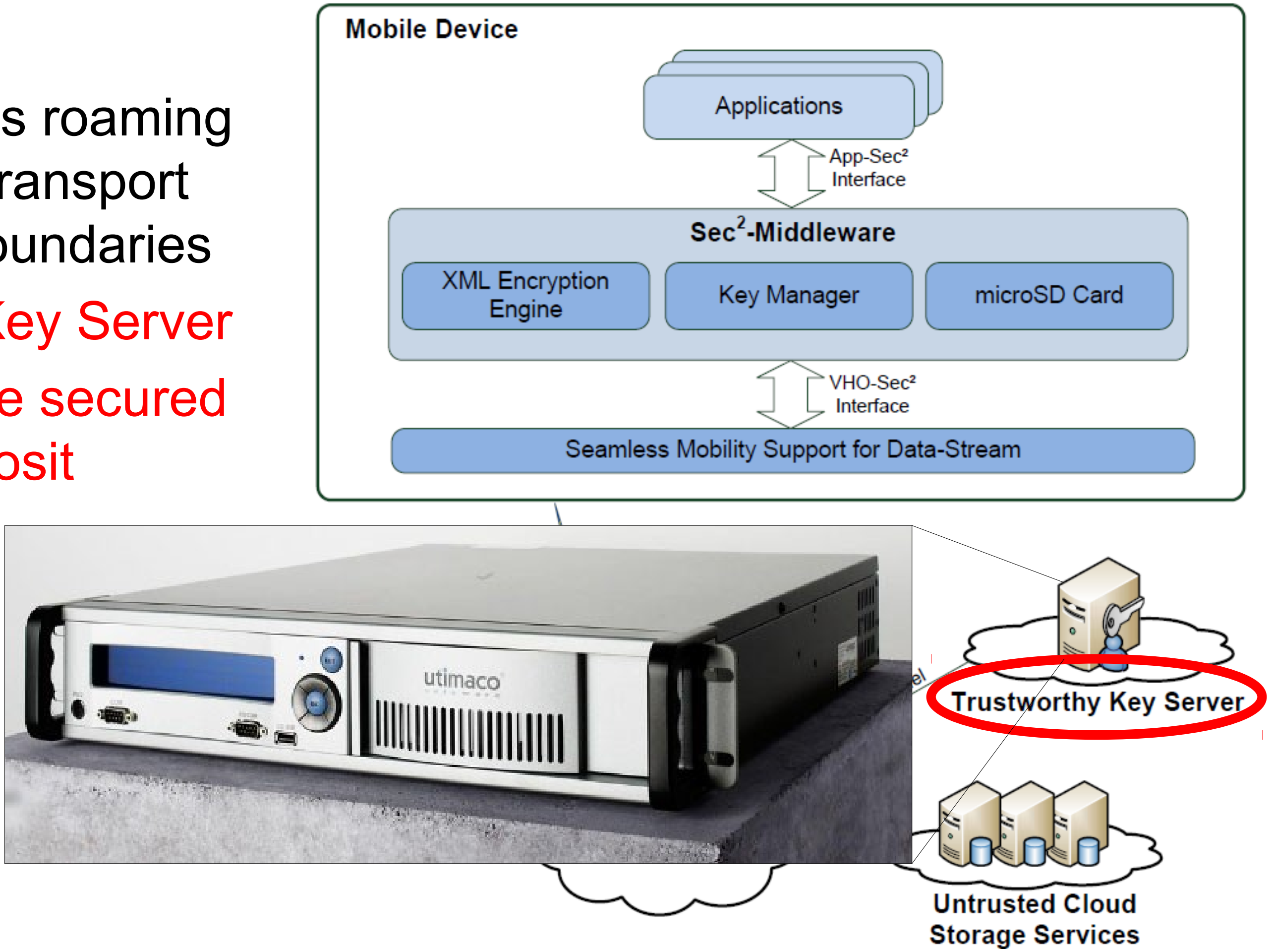
- VHO Layer
  - Seamless roaming beyond transport media boundaries



Sec² Architecture

Module Scheme 2/2

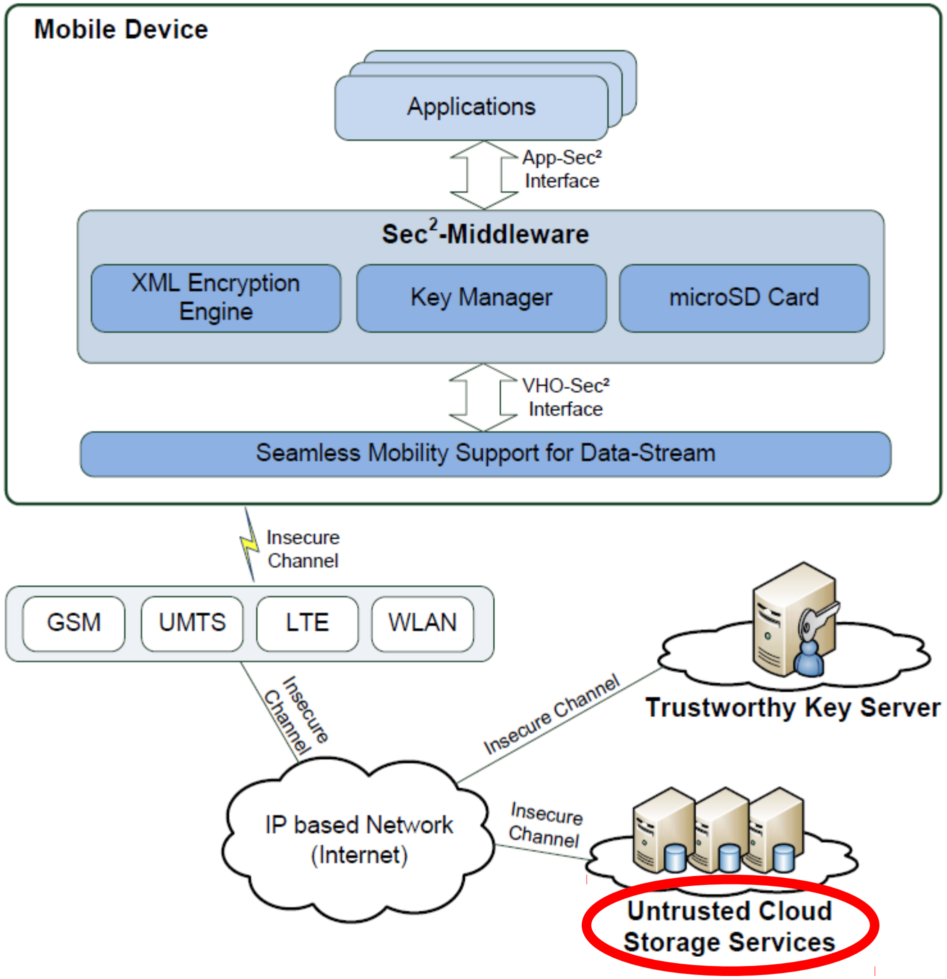
- VHO Layer
  - Seamless roaming beyond transport media boundaries
- Trustworthy Key Server
  - Hardware secured key deposit



Sec² Architecture

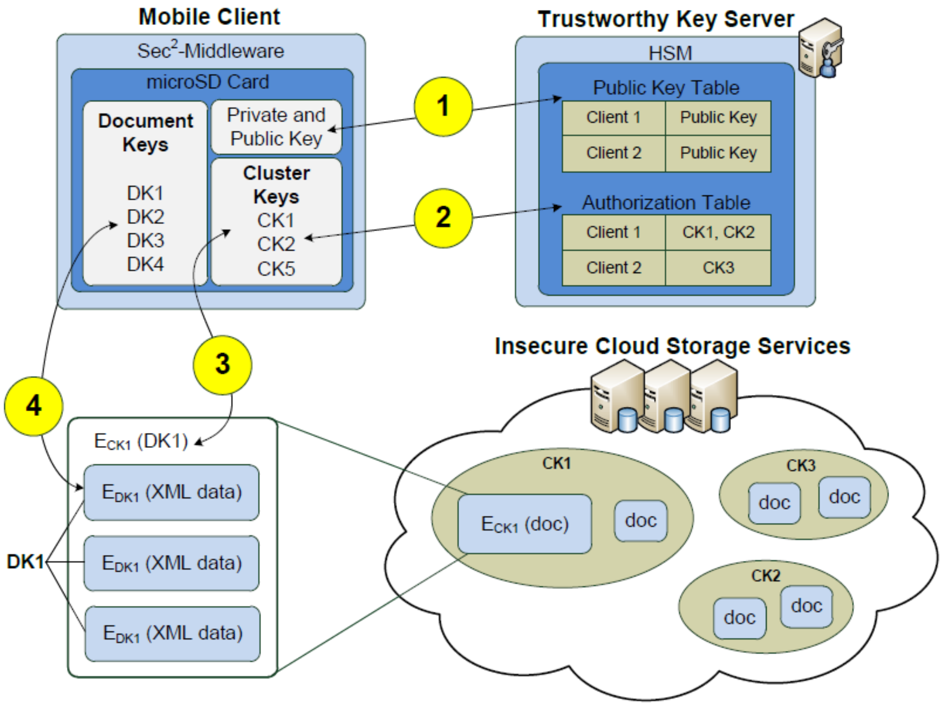
Module Scheme 2/2

- VHO Layer
  - Seamless roaming beyond transport media boundaries
- Trustworthy Key Server
  - Hardware secured key deposit
- Untrusted Cloud Storage Service
  - Storage for data



Sec² Architecture

Multi Stage Key Concept



Public Key Table

Client 1	Public Key
Client 2	Public Key

Authorization Table

Client 1	CK1, CK2
Client 2	CK3

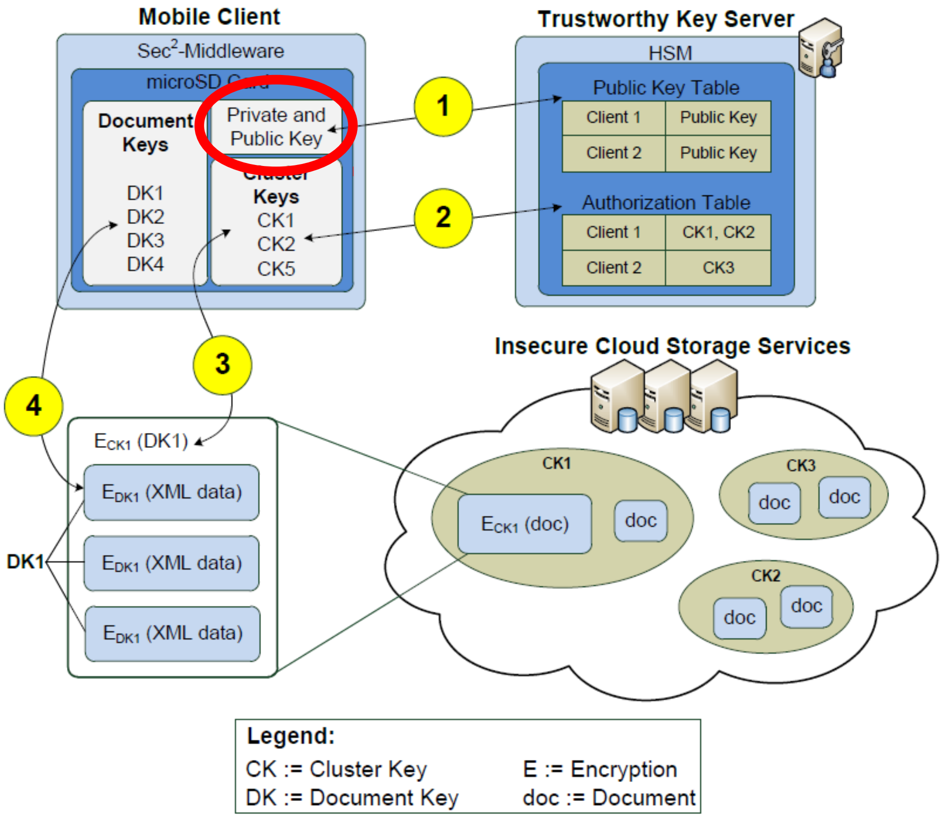
Legend:

CK := Cluster Key
DK := Document Key
E := Encryption
doc := Document

Sec² Architecture

Multi Stage Key Concept

- (asym) Private/Public key
  - Authentication
  - Key wrap
  - User specific



Public Key Table

Client 1	Public Key
Client 2	Public Key

Authorization Table

Client 1	CK1, CK2
Client 2	CK3

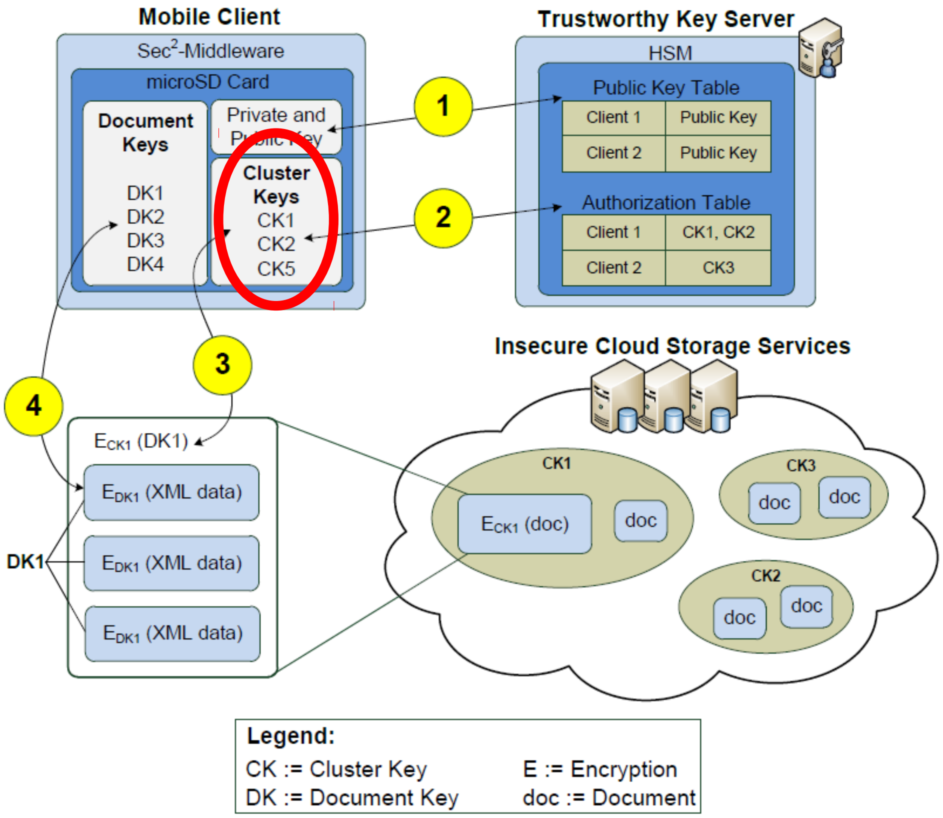
Legend:

CK := Cluster Key	E := Encryption
DK := Document Key	doc := Document

Sec² Architecture

Multi Stage Key Concept

- (asym) Private/Public key
  - Authentication
  - Key wrap
  - User specific
- (sym) Cluster key
  - Document key wrap
  - Group specific



Public Key Table

Client 1	Public Key
Client 2	Public Key

Authorization Table

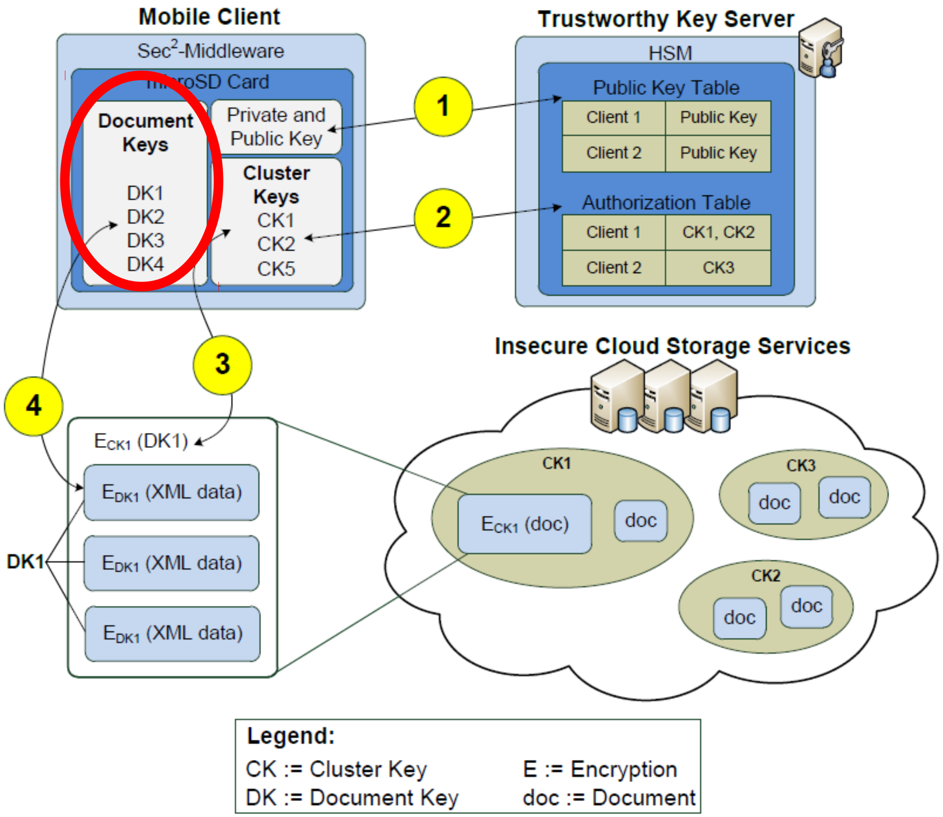
Client 1	CK1, CK2
Client 2	CK3

Legend:
CK := Cluster Key
DK := Document Key
E := Encryption
doc := Document

Sec² Architecture

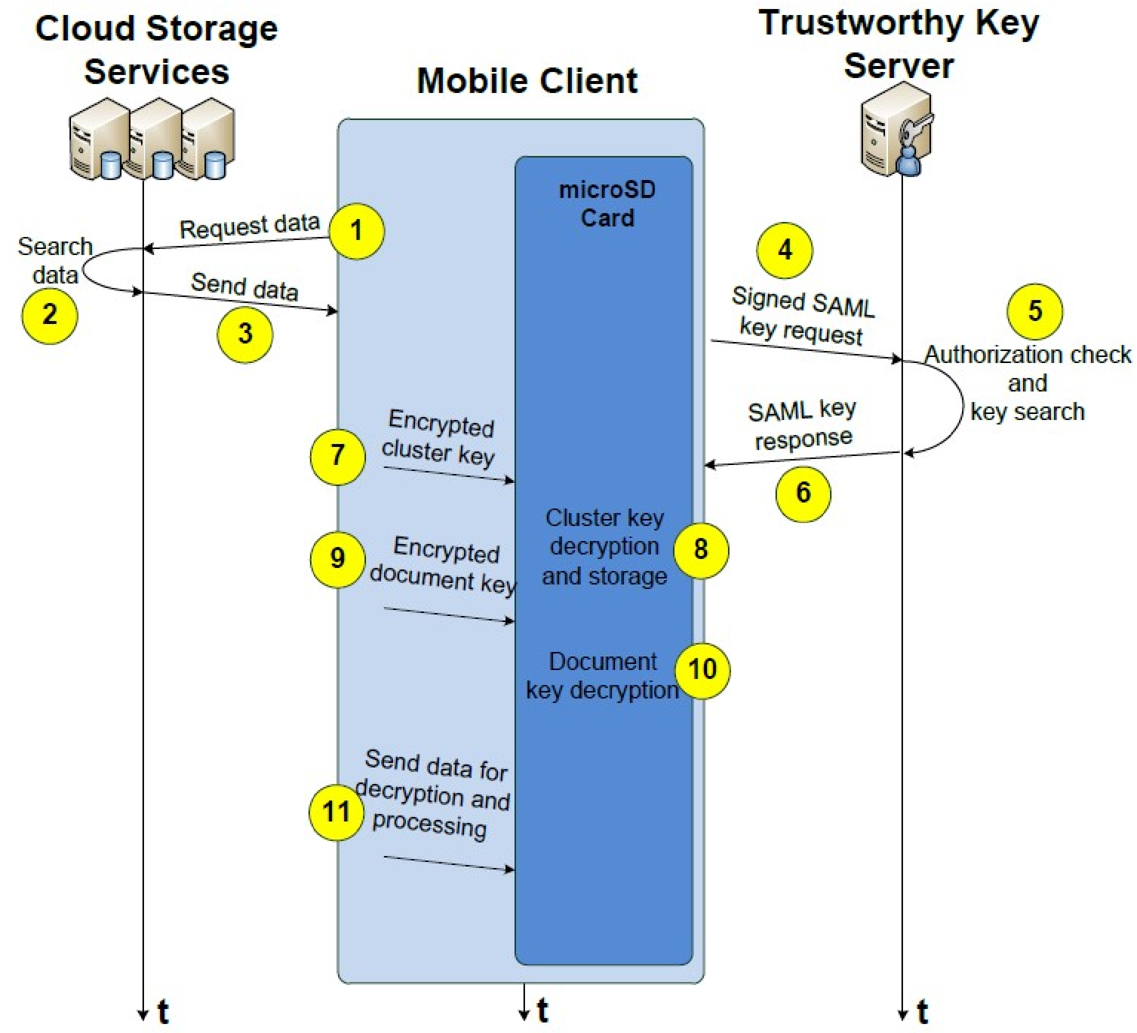
Multi Stage Key Concept

- (asym) Private/Public key
  - Authentication
  - Key wrap
  - User specific
- (sym) Cluster key
  - Document key wrap
  - Group specific
- (sym) Document key
  - Payload en-/decryption



Sec² Architecture

Communication Example



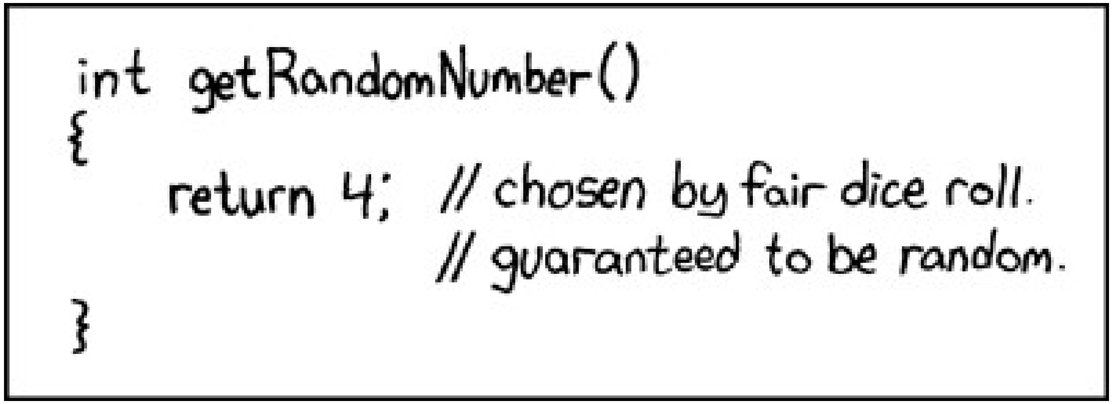
Time for discussion...

… time for your questions

SPONSORED BY THE

Federal Ministry
of Education
and Research

This work was funded by the **Sec2** project of the **German Federal Ministry of Education and Research** (BMBF, FKZ: 01BY1030)



```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Source: [www.xkcd.com]

Sec2
www.sec2.org

Christopher Meyer
christopher.meyer@rub.de
www.nds.rub.de