3GPP TSG SA WG3 Security **S3-010530**

October 16-19, 2001

Sydney, Australia

Agenda Item: 5.1

Source: Ericsson

Title: Application Level Security Framework for Terminals

Document for: Information

1. Scope and objectives

T groups, but T2 in particular have been lately looking into the security implications that several applications might have in terminals. These applications includes MExE, User Profiles, Device Management, Digital Rights Management, … and according to T2 the required security mechanisms implies the support for access control, privacy, PKI (certificate handling), etc…

This is why these groups are talking about a so called "General Application Security Framework for Terminals". The attached document includes a presentation to T2 where this concept is introduced and a way forward in order to accomplish this work is proposed.

The presentation of this concept at S3#20 is intended to be the starting point of discussions on this matter at S3. It should be also considered as the starting point of co-operation with T groups in order to agree on the best way to accomplish the related work.

3GPP TSG-T2 #14
Edinburgh, Scotland
3-7 September 2001

T2-010651

THE CONTINUED WORK WITH APPLICATIONS

AND A SECURITY FRAMEWORK

Gunilla Bratt

Ericsson

PRESENT CONCERNS FOR APPLICATION DEPLOYMENT

- **To ensure a successful deployment of 3G, several (application independent) mechanisms of *infrastructure type* must be developed to enable *secure, interoperable and portable* applications.**

- **For handling of capabilities and preferences a work on User Profiles is ongoing and includes**
  - **Description, organization (categorisation), and distribution of the profiles**
  - **Security and privacy**

- **Management mechanisms are needed and will require access control.**

- **Access control mechanisms are required in the UE, not only for MExE, to ensure the security and privacy.**

- **Further mechanisms include a PKI and relevant formats (such as for certificates and signatures) need unambiguous definitions.**

THE WAY FORWARD

- Without general mechanisms several problems will arise, e.g.:
  - Several different standards, requiring parallel implementations in the UE, to a higher expense and less testability.
  - Lacking interoperability and portability.
  - Storage congestion on the USIM due to too many RPK.

- There is a need in 3GPP for a general Application Level Security Framework and T2 has a responsibility to take!

APPLICATION LEVEL SECURITY FRAMEWORK IN 3GPP

- Common mechanisms to be specified in 3GPP must include
  - Access control mechanisms
    - Objects (e.g. for management and helpdesk purposes)
    - Functions (e.g. MExE actions)
    - The MExE concepts can be reused
  - Alignment of formats and mechanisms for PKI
    - Certificate format
    - Signature format
    - PKI adaptations and amendments:
      - Certificate download mechanisms
      - Certificate storage mechanisms
      - Certificate chain verification
      - Certificate revocation

STANDARDISATION STRATEGY

- RELEASE 5 - SHORT TERM

- Alignment of MExE and WAP
  - WAP Cert Profile
  - WAP Signed Content Signature format
  - PKI alignment
  - Certificate storage mechanisms

- MExE specific
  - Unique certification path
  - Domain identification
  - RPK sharing
  - Signed un-trusted as well as un-trusted (and no domains)
    - Shorter time to market
    - “Web” aligned principle

- RELEASE 6 - LONG TERM

- New TS(s) for Application Level Security Framework (independent of MExE)
  - Remove all generics from MExE
  - “Include” relevant WAP specs
  - Access control mechanisms

  - The new TS includes
    - Certificate revocation
    - 3GPP Cert Profile
    - 3GPP Signed Content Signature format
    - PKI framework
    - Certificate storage mechanisms