Status Report T3

Dr. Klaus Vedder
Chairman T3

TSG-T #9

Hawaii, 20 - 22 September 2000

Giesecke & Devrient

Documents

- TP-000145: Status Report to TSG-T #9 (this document)
- TP-000146: CR to GSM 03.19 *SIM API - stage 2 - (Java^{TM})*
- TP-000147: CRs to GSM 03.48 *SIM toolkit secure messaging*
- TP-000148: CRs to GSM 11.11 *SIM-ME interface*
- TP-000149: CRs to GSM 11.14 *SIM Application Toolkit*
- TP-000150: CR to TS 21.111 *USIM and IC card requirements*
- TP-000151: CR to TS 31.101 *UICC-Terminal Interface*
- TP-000152: CRs to TS 31.102 *USIM application*
- TP-000153: CR to TS 31.110 *Application Identifiers*
- TP-000154: CRs to TS 31.111 *USIM Application Toolkit*
- TP-000155: New Work Items
- TP-000156: TS 31.120 *UICC-terminal interface; Physical and logical tests*
- TP-000157: TS 31.121 *UICC-terminal interface; USIM application tests*
- TP-000158: TS 31.122 *USIM conformance Test specification*
- TP-000159: CR 03.19-A004: Correction of the AID coding for the API packages

Giesecke & Devrient

ETSI EP SCP #2

- Meeting hosted by LG InFocom, San Diego, 21 - 24 August 2000

- Election of Chairman and Vice-chairmen
  - Chairman: Dr. Klaus Vedder, Giesecke & Devrient
  - Vice-chairs: Nigel Barnes, Motorola
                Mark Hosford, LG InFocom

- New name: EP SCP (Smart Card Platform)

- Approval of TS 102 221 for publication as Release 99
  - formerly TS 31.101 the contents of which had been transferred to EP SCP
  - several Release 99 CRs including selection by partial AID were incorporated

Giesecke & Devrient

EP SCP #2

Four new work items

- Technology Independent Card Application Toolkit
  - a Card Application Toolkit for the common smart card platform

- Common application identifier specification
  - merging of existing work (e.g. ETSI TS 101 220 and 3G TS 31.110) plus specifying (or reserving) particular identifiers for specific e-commerce transaction types

- Enhancement to administrative commands
  - support for the existing mechanisms in GSM 03.48 (Secure messaging) and other specifications to be identified. In particular, key management could be provided for PKI technology

- Core API and secure messaging feasibility study
  - common core secure messaging syntax and semantics across first level application execution environments

Giesecke & Devrient

Meetings

- ● TSG-T3 #15
  - ❍ 16 - 18 August 2000, San Diego, hosted by LG Infocom
    attended by 63 delegates from 11 countries
  - ❍ followed by EP SCP #2 (formerly "newSMG9"), 21-24 August 2000

- ● Ad hoc meetings
  - ❍ #7   JAVA API testing (Oberthur, Paris)
  - ❍ #8   USIM Toolkit interpreter (Giesecke & Devrient, Munich)
  - ❍ #9   SIM Toolkit testing (KPN Orange Belgium, Brussels)
  - ❍ #10 WAP-SAT interaction, joint meeting with WAP Forum (Motorola, Winchester)
  - ❍ #11 JAVA API testing (Gemplus, Marseille)
  - ❍ #13 USIM Toolkit interpreter (Vodafone, Newbury)

Giesecke & Devrient

CRs to GSM 03.19 and GSM 03.48

- GSM 03.19 *SIM Applic. Programm. I/f (API) - stage 2 - (Java^{TM})*
  - CR to Release 98 in TP-000146
    - A003: Definition of the value of the getShareableInterfaceObject() method byte parameter for the Toolkit Interface
  - CR to Release 98 in TP-000159
    - A004: Correction of the AID coding for the API packages

    NOTE: This CR was not discussed at the T3 Plenary,
    it was agreed by seven card manufacturers just prior to T #9

- GSM 03.48 *SIM toolkit secure messaging (stage 2)*
  - CRs to Release 99 in TP-000147
    - A012: Modification of the fields to be included in the 03.48 response packet checksum computation
    - A013: Clarification of the KID and KIC fields for Open Platform keys
    - A014: Clarific. on Access Domain param. in Install(Install) command

Giesecke & Devrient

CRs to GSM 11.11 and GSM 11.14

- **GSM 11.11** *SIM - ME interface*
    - CRs to Release 99 in TP-000148
        - A125: Warning regarding network selection with access technology
        - A126: Standardise the current GAIT commands and reserving these CLA/INS codes

- **GSM 11.14** *SIM Application Toolkit*
    - CRs to Release 98 and 99 in TP-000149
        - A183 R98, A184 R99:
          Clarification for Alpha Identifier in PLAY TONE
        - A185 R98, A186 R99:
          EVENT DOWNLOAD-MT call : correction of the sub-address description
        - A187 R98, A188 R 99:
          Correction to GET INPUT regarding number of response string variables

Giesecke & Devrient

CRs to TSs 21.111, 31.101 and 31.110

- **21.111** *USIM and IC Card Requirements*
  - CR to Release 99 in TP-000150
    - 005: Partial AID selection requirements

- **31.101** *UICC-Terminal I/f; Physical & Logical Characteristics*
  - CR to Release 99 in TP-000151
    - 023: Replacement of the techincal contents with a reference to TS 102 221

- **31.110** *Numbering system for telecommunication IC card applications*
  - CR to Release 99 in TP-000153
    - 003 r1: Reservation of TAR values

Giesecke & Devrient

CRs to TS 31.102
Characteristics of the USIM Application

- Corrections to Release 99 in TP-000152
  - 044 r1: Correction to call information access conditions and correction of DF_GSM file IDs
  - 045: Clarification of the type 3 links of the phonebook
  - 046: Alignment of EF(CCP2) with EF(ECCP)
  - 047 r1: General corrections
  - 048: APN Control List coding
  - 049: Alignment with TS 33.102 regarding authentication Sequence Numbers
  - 050: Preferred language selection
  - 051: Application Selection by partial AID
  - 052: Addition of warning regarding network selection with access technology
  - 053: Phone book clarifications

Giesecke & Devrient

CRs to TS 31.111
USIM Application Toolkit (USAT)

- Corrections to R99 and Release 2000 issues in TP-000154
  - 005 R99: Correction of Profile Download regarding USAT service table
  - 006 R00: Modification of GET INKEY
  - 007 R00: Suppression of DTMF tones during hidden input
  - 008 R99: Correction to GET INPUT regarding number of response string variables
  - 009 R99: Clarification for Alpha Identifier in PLAY TONE
  - 010 R99: EVENT DOWNLOAD-MT call : correction of the sub-address description
  - 011 R00: Addition of a Technology Indicator Tag in a Terminal Response message

Giesecke & Devrient

Test Specifications

- Test following draft versions of Release 99 test specifications are presented for information and comment

  - TS 31.120 v1.0.0 in TP-000156
    UICC-terminal interface; Physical and logical tests

  - TS 31.121 v1.0.0 in TP-000157
    UICC-terminal interface; USIM application tests

  - TS 31.122 v1.0.0 in TP-000158
    USIM conformance test specification

  The draft documents were developed by MCC Task 162

  T3 reviewed the work of MCC Task 162 and endorsed the approach taken so far

  T3 then approved the draft versions for presentation to TSG-T #9

  They will be presented for approval to TSG-T #10

- T3 #15 approved a CR to GSM 11.10-4 (SIM Application Toolkit tests) to be forwarded to GERAN

Giesecke & Devrient

USIM API Test Specification

- **Test specification for the USIM API**
  - WI approved by TSG-T #7
  - discussion with SUN about laying open the JavaCard™ 2.1 Compliance Test Suite (CJCK)
  - to be presented to TSG-T #10 for information

- **T3 #15 clarified that**
  - a test specification shall not contain a reference to a non-public specification or document nor to any other non-public material
  - a test specification shall not contain any requirements, it shall only contain tests for requirements in its core specification

Giesecke & Devrient

New Work Items (TP-000155)

- Work item description: "Multos API"
  - to allow the use of a further API in addition to JAVA™ API (GSM 03.19)
  - MULTOS API will be based on GSM 02.19
  - output: new specification and new test specification for Release 2001
  - the API would be based on the Release 2000 USIM Toolkit specification
  - both specifications to TSG-T for information / approval: T #11 / T #12

- Work item description: "USAT local link"
  - to allow the use of other bearers such as RS232, Bluetooth
  - output: CRs to 31.111 and, possibly, to GSM 03.48
  - secodary responsibility: TSG-T2
  - CRs for approval by TSG-T: T #10

Giesecke & Devrient

Other Issues

- WP *Application Protocol Interface (API)* was established
    - Paul Jolivet, NTT DoCoMo Europe, was elected as the WP Chair

- T3 thanked the outgoing rapporteurs Kristian Woodsend and Rune Lindholm for all their work over the years in advancing GSM 11.11 / TS 31.111 and TS 31.101

- Support of USIM (security) functionality by GSM only R99 MEs
    - LS to S3 contained in T3-000470; answer in TP-000170
    - S3 will align its specifications with the T3 assumption that a R99 GSM only ME need not support a USIM (wrt security functionality)

Giesecke & Devrient

Other Issues ctd.

- WI Standardisation of USIM Toolkit interpreter
  - stage 1 nearly completed by ad hoc meeting this week
  - byte codes laid open by SIM Alliance and Across Wireless
  - specifications to TSG-T #10 for information

- Request by SIM Alliance for formal liaison with T3

- T3 is concerned about R2000 work items developed by other groups which will require USIM support and may only be finalised towards the end of the year (VHE user profiles, IP multi-media services)

Giesecke & Devrient

Meeting Calendar

- ## TSG-T3 #16

  - 13 - 15 November 2000, Seoul, hosted by Samsung
    followed by EP SCP #3 (15 -17 November 2000)

- ## TSG-T3 #17

  - 15 - 17 January 2001, Berlin, hosted by ORGA
    followed by EP SCP #4 (17 -19 January 2001)

    date and venue subject to confirmation

- ## TSG-T3 #18

  - 26 - 28 February 2001, Sophia-Antipolis, hosted by ETSI
    followed by EP SCP #5 (28 Feb. - 02 March 2001)

    meeting, *date and venue subject to confirmation*

- Confirmed invitations received from: Gemplus (spring 2001);
  T1 (summer ?); Toshiba, Fujitsu, Hitachi and DNP (November 2001)

Giesecke & Devrient

Decisions Required

- Approval of CRs to GSM 03.19 (TP-000146 and TP-000159)

- Approval of CRs to GSM 03.48 (TP-000147)

- Approval of CRs to 11.11 (TP-000148)

- Approval of CRs to 11.14 (TP-000149)

- Approval of CR to TS 21.111 (TP-000150)

- Approval of CR to TS 31.101 (TP-000151)

- Approval of CRs to TS 31.102 (TP-152)

- Approval of CR to TS 31.110 (TP-000153)

- Approval of CRs to TS 31.111 (TP-000154)

- Approval of new Work Items (TP-000155)

- Liaison with SIMalliance

Giesecke & Devrient